

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 1月13日

出 願 番 号
Application Number:

特願2000-004271

出 願 人
Applicant(s):

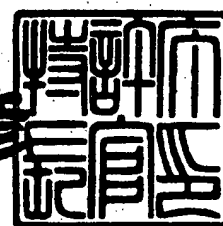
カシオ計算機株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 4月 7日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3024176

【書類名】 特許願

【整理番号】 99-2069-00

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/00
G06F 12/14

【発明者】

【住所又は居所】 東京都羽村市栄町3丁目2番1号
カシオ計算機株式会社羽村技術センター内

【氏名】 大塚 基

【特許出願人】

【識別番号】 000001443

【氏名又は名称】 カシオ計算機株式会社

【代理人】

【識別番号】 100074985

【弁理士】

【氏名又は名称】 杉村 次郎

【手数料の表示】

【予納台帳番号】 023180

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9109737

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ管理システムおよびそのプログラム記録媒体

【特許請求の範囲】

【請求項 1】

携帯端末装置と、この携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置とを有し、

サーバ装置は、携帯端末装置にて利用されるレコード群をマスタデータファイルから切り出し、その切り出したレコード群からモバイルデータファイルを作成するモバイルデータ作成手段と、

携帯端末装置との対応付けが設定されているデータ記憶媒体に前記モバイルデータ作成手段によって作成されたモバイルデータファイルを書き込む書込手段とを具備し、

携帯端末装置は、それにセットされているデータ記憶媒体が当該端末に対応付けられている正当な媒体かを判別する判別手段と、

この判別手段によって当該端末対応の媒体であることが判別された場合に、そのデータ記憶媒体内のモバイルデータファイルへのアクセスを許可するアクセス制御手段とを具備したことを特徴とするセキュリティ管理システム。

【請求項 2】

前記モバイルデータ作成手段は、携帯端末装置にて利用されるレコード群をマスタデータファイルから切り出す際に、その携帯端末装置側での処理内容に合わせて予め設定されているレコード抽出条件を参照し、このレコード抽出条件に合致するレコード群を切り出すようにしたことを特徴とする請求項 1 記載のセキュリティ管理システム。

【請求項 3】

前記モバイルデータ作成手段は、携帯端末装置にて利用されるレコード群をマスタデータファイルから切り出してモバイルデータファイルを作成する際に、その携帯端末装置側での処理内容に合わせて予め設定されている抽出対象フィールドを参照し、この抽出対象フィールドの条件に合致するフィールドのみからなるレコード構成のモバイルデータファイルを作成するようにしたことを特徴とする

請求項1あるいは2記載のセキュリティ管理システム。

【請求項4】

前記モバイルデータ作成手段は、携帯端末装置にて利用されるレコード群をマスターデータファイルから切り出す際に、書き込み対象のデータ記憶媒体内に設定されている識別情報を取得し、この識別情報に基づいてマスターデータファイルを決定制すると共に、このマスターデータファイルからレコード群を切り出すための切り出し条件を決定し、決定したマスターデータファイルからその切り出し条件にしたがってレコード群の切り出しを行うようにしたことを特徴とする請求項1記載のセキュリティ管理システム。

【請求項5】

携帯端末装置によって利用されるデータ記憶媒体にモバイルデータファイルを書き込んで配布するサーバ装置は、

モバイルデータファイル进行处理するためのアプリケーションソフトが当該モバイルデータファイルに対応付けてデータ記憶媒体内に記憶されているかを判別する判別手段を設け、

この判別手段によってそのアプリケーションソフトが記憶されていないことが判別された場合には、当該モバイルデータファイルに対応付けてそれ进行处理するためのアプリケーションソフトをデータ記憶媒体内に書き込むようにしたことを特徴とする請求項1記載のセキュリティ管理システム。

【請求項6】

前記データ記憶媒体内にモバイルデータファイルに対応付けてそのアプリケーションソフトが記憶されている場合に、そのアプリケーションソフトは最新のものかを判別するアプリケーション判別手段と、

この判別手段によって最新のアプリケーションソフトではないことが判別された場合に、前記データ記憶媒体内にモバイルデータファイルに対応付けて記憶されているアプリケーションソフトを最新のアプリケーションソフトに書き換えるアプリケーション更新手段とを設けたことを特徴とする請求項5記載のセキュリティ管理システム。

【請求項7】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、
携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置に対して、

携帯端末装置にて利用されるレコード群をマスタデータファイルから切り出し、その切り出したレコード群からモバイルデータファイルを作成させるコンピュータが読み取り可能なプログラムコードと、

携帯端末装置との対応付けが設定されているデータ記憶媒体に前記モバイルデータファイルを書き込ませるコンピュータが読み取り可能なプログラムコードと

携帯端末装置に対して、それにセットされているデータ記憶媒体が当該端末に対応付けられている正当な媒体かを判別させるコンピュータが読み取り可能なプログラムコードと、

当該端末対応の媒体であることが判別された場合に、そのデータ記憶媒体内のモバイルデータファイルへのアクセスを許可させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

この発明は、携帯端末装置によって可搬型データ記憶媒体にアクセスする際のセキュリティ対策を講じたセキュリティ管理方法およびそのプログラム記録媒体に関する。

【 0 0 0 2 】

【従来の技術】

近年、コンパクトディスクやメモリカード等の可搬型記憶媒体は、大容量化、小型化が進み、大量のデータベースを可搬型記憶媒体に格納することによって、各種のデータベースを自由に持ち運びことができるようになってきている。ここで、営業担当者が携帯端末装置を持参して、日常の営業活動を行う場合において、携帯端末装置はその内蔵メモリの容量が少ないために、各種業務処理用のデータベースの一部あるいは全部を可搬型記憶媒体に格納するようにしている。ここ

で、営業担当者は、端末本体に可搬型記憶媒体を装着し、外出先でその記憶内容をアクセスして表示出力させたり、データ更新等を行うようにしている。この場合、携帯端末装置によって可搬型データ記憶媒体をアクセスする際のセキュリティ対策としては、入力されたパスワードによって正当な端末利用者かを認証するようにしている。

【0003】

【発明が解決しようとする課題】

ところで、本来、個人専用機としての携帯端末装置においても、正社員の他、派遣社員、パート、アルバイトの方も使用するケースが増えてきている。また、携帯端末装置は、外出先に持ち運んで使用するという関係上、可搬型記憶媒体や携帯端末装置自体を外出先で紛失したり、盗難される危険性があった。したがって、可搬型記憶媒体や端末の内蔵メモリ内に、機密性の高い重要な企業情報や個人情報格納されている場合に、紛失、盗難、悪意によって、その重要情報が他人に漏洩されるおそれは極めて高かった。

すなわち、従来においては、携帯端末装置を主に外出先で使用するという関係上、入力操作を複雑化した厳密なセキュリティ管理よりも、操作の簡素化、迅速性等の操作環境を重視しているため、可搬型記憶媒体や携帯端末装置の紛失や盗難に対するセキュリティ対策や派遣社員、パート等による悪意に対するセキュリティ対策は、十分ではなく、ユーザパスワードを知っていれば、あるいはパスワードの偶発的なヒットによって、誰でも、どのパソコンからでも容易に携帯端末や記憶媒体内のデータをアクセスすることができ、重要情報が他人に漏洩してしまう危険性は、極めて高かった。また、ユーザ設定によって、任意にセキュリティ対策を講じるための仕組みを携帯端末装置自体に持たせておくことは、逆に、第3者によってその設定部分の変更も容易に行える危険性を含むことになり、その仕組み自体が安全性を損なう要因となってしまう。

この発明の課題は、可搬型データ記憶媒体に対するセキュリティ管理を確実なものとするために、データ記憶媒体へのデータファイルの書き込みの他、データ記憶媒体とそれをアクセス可能な携帯端末装置との対応付けをサーバ装置が一括して行うことができると共に、元となるマスタデータベースをそのまま書き込

むのではなく、マスタデータベースから切り出したレコード群のみからなるモバイルデータファイルを作成して書き込むことで、当該媒体対応の正当な端末に対しても必要以上の情報を提供しないという対策を講じることができ、また、紛失、盗難、悪意等によるデータ記憶媒体内の重要情報の漏洩を確実に防止できるようになることである。

【0004】

この発明の手段は、次の通りである。

請求項第1記載の発明は、携帯端末装置と、この携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置とを有し、サーバ装置は、携帯端末装置にて利用されるレコード群をマスタデータファイルから切り出し、その切り出したレコード群からモバイルデータファイルを作成するモバイルデータ作成手段と、携帯端末装置との対応付けが設定されているデータ記憶媒体に前記モバイルデータ作成手段によって作成されたモバイルデータファイルを書き込む書込手段とを具備し、携帯端末装置は、それにセットされているデータ記憶媒体が当該端末に対応付けられている正当な媒体かを判別する判別手段と、この判別手段によって当該端末対応の媒体であることが判別された場合に、そのデータ記憶媒体内のモバイルデータファイルへのアクセスを許可するアクセス制御手段とを具備するものである。

なお、この発明は次のようなものであってもよい。

(1) 前記モバイルデータ作成手段は、携帯端末装置にて利用されるレコード群をマスタデータファイルから切り出す際に、その携帯端末装置側での処理内容に合わせて予め設定されているレコード抽出条件を参照し、このレコード抽出条件に合致するレコード群を切り出す。

(2) 前記モバイルデータ作成手段は、携帯端末装置にて利用されるレコード群をマスタデータファイルから切り出してモバイルデータファイルを作成する際に、その携帯端末装置側での処理内容に合わせて予め設定されている抽出対象フィールドを参照し、この抽出対象フィールドの条件に合致するフィールドのみからなるレコード構成のモバイルデータファイルを作成する。

(3) 前記モバイルデータ作成手段は、携帯端末装置にて利用されるレコード

群をマスタデータファイルから切り出す際に、書き込み対象のデータ記憶媒体内に設定されている識別情報を取得し、この識別情報に基づいてマスタデータファイルを決定すると共に、このマスタデータファイルからレコード群を切り出すための切り出し条件を決定し、決定したマスタデータファイルからその切り出し条件にしたがってレコード群の切り出しを行う。

(4) 携帯端末装置によって利用されるデータ記憶媒体にモバイルデータファイルを書き込んで配布するサーバ装置は、モバイルデータファイル进行处理するためのアプリケーションソフトが当該モバイルデータファイルに対応付けてデータ記憶媒体内に記憶されているかを判別する判別手段を設け、この判別手段によってそのアプリケーションソフトが記憶されていないことが判別された場合には、当該モバイルデータファイルに対応付けてそれ进行处理するためのアプリケーションソフトをデータ記憶媒体内に書き込む。

(5) 前記データ記憶媒体内にモバイルデータファイルに対応付けてそのアプリケーションソフトが記憶されている場合に、そのアプリケーションソフトは最新のものをかを判別するアプリケーション判別手段と、この判別手段によって最新のアプリケーションソフトではないことが判別された場合に、前記データ記憶媒体内にモバイルデータファイルに対応付けて記憶されているアプリケーションソフトを最新のアプリケーションソフトに書き換えるアプリケーション更新手段とを設ける。

したがって、請求項第1記載の発明においては、可搬型データ記憶媒体に対するセキュリティ管理を確実なものとするために、データ記憶媒体へのデータファイルの書き込みの他、データ記憶媒体とそれをアクセス可能な携帯端末装置との対応付けをサーバ装置が一括して行うことができると共に、元となるマスタデータベースをそのまま書き込むのではなく、マスタデータベースから切り出したレコード群のみからなるモバイルデータファイルを作成して書き込むことで、当該媒体対応の正当な端末に対しても必要以上の情報を提供しないという対策を講じることができ、また、紛失、盗難、悪意等によるデータ記憶媒体内の重要情報の漏洩を確実に防止することができる。

【0005】

【発明の実施の形態】

以下、図 1 ～ 図 1 7 を参照してこの発明の一実施形態を説明する。

図 1 は、この実施形態におけるセキュリティ管理システムの全体構成を示したブロック図である。

このセキュリティ管理システムは、例えば、会社組織において会社側に設置させているサーバ装置 1 と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末装置） 2 と、この携帯端末装置 2 にセットされて利用される可搬型記憶媒体 3 とを有している。そして、サーバ装置 1 側で記憶管理されているアプリケーションソフト／データベース等を持ち運び自在な可搬型記憶媒体 3 を介して携帯端末装置 2 側に外部提供するようにしており、この記憶媒体 3 にデータベース等を書き込んで端末装置へ配布する際に、サーバ装置 1 は当該端末と記憶媒体とを対応付けるための情報を設定したり、各種のセキュリティ対策を講じることによって、記憶媒体 3 内のアプリケーションソフト／データベース等が第三者によって不正コピーされたり、情報が漏洩されることを確実に防止するようにしたものである。

【0 0 0 6】

そして、各営業担当者は、外出先で可搬型記憶媒体 3 内のアプリケーションソフト／データベースをアクセスしながら営業活動を行い、そして、1日の営業終了時に端末本体から可搬型記憶媒体 3 を抜き取り、それをサーバ装置 1 側のカードリーダー／ライタ 4 にセットすると、サーバ装置 1 はカードリーダー／ライタ 4 を介して記憶媒体 3 内の営業記録を収集処理するようにしている。

そして、サーバ装置 1 と複数台の携帯端末装置 2 とはシリアルケーブル 5 を介して着脱自在に接続可能となっている。

【0 0 0 7】

可搬型記憶媒体 3 は、各種業務処理用のアプリケーションソフトやデータベース等を記憶するもので、例えば、コンパクトフラッシュカードによって構成されている。以下、可搬型記憶媒体 3 をモバイルデータベースカード（DBカード）と称する。ここで、図中、各 DB カード 3 に付した「# A」「# B」、「# C」、……は、端末名称「A」、「B」、「C」、……で示される携帯端末装置 2 に

対応付けられた端末対応のカードであることを示している。なお、この実施形態においては端末対応のカードの他、後述する端末グループ対応のカードも存在するが、図1の例では端末対応のカードのみを示している。カードリーダー/ライター4はDBカード3を複数枚同時にセット可能なもので、複数のカード挿入口を有している。

そして、サーバ装置1はDBカード3を介して携帯端末装置2側にアプリケーションソフト/データベースファイル（APソフト/DBファイル）を配布する。すなわち、サーバ装置1はDBカード3に書き込む書込対象、つまり、配布対象のAPソフト/DBファイルを呼び出してカードリーダー/ライター4に与え、それにセットされている1または2以上のDBカード3にAPソフト/DBファイルを書き込む。

【0008】

図2は、例えば、業務グループ「営業1課」、「営業2課」、「プロジェクトA」、「プロジェクトB」、……に対応付けた端末グループと、この端末グループ対応のDBカード3との関係を示すと共に、端末とユーザとの対応関係を示したものである。すなわち、図中、「#A1」、「#A2」、「#A3」で示す各DBカード3は、端末名称が「A1」、「A2」、「A3」である各携帯端末装置2が属する端末グループA対応の記憶媒体であり、同様に、「#B1」、「#B2」……で示す各DBカード3は、端末名称が「B1」、「B2」、……である各携帯端末装置2が属する端末グループB対応の記憶媒体であり、同一グループ内の各DBカード3はそのグループに属する各携帯端末装置2で共通して使用することができるようになっている。

【0009】

また、ある携帯端末を利用することができる権限を有するユーザは、一人に限らず、複数のユーザが一台の携帯端末装置を共有して使用することができ、また、あるユーザは複数台の携帯端末装置を利用することができる権限を有している。例えば、端末グループAにおいて、端末名称「A1」で示される携帯端末装置と、ユーザ「UA1」～「UA4」との対応関係が定義され、また、端末名称「A2」で示される携帯端末装置と、ユーザ「UA1」～「UA3」との対応関係

が定義されており、これらの間に限り利用関係があることを示している。この場合、複数ユーザによる共有使用が可能な端末対応の各DBカードには、共有使用が可能な各ユーザに対応して、その認証情報（パスワード）が設定される。

【0010】

図3は、この実施形態の特徴である多重セキュリティ管理の仕組みを概念的に示した図である。この多重セキュリティ管理は、携帯端末装置2が任意のDBカードをアクセスする際、あるいはDBカード3が任意の端末装置によってアクセスされる際のセキュリティ処理を示したもので、この多重セキュリティを大別すると、4つのセキュリティ層からなる。

すなわち、この多重セキュリティ管理の仕組みは、第1セキュリティ層（DBカードセキュリティ）と、第2セキュリティ層（パスワード認証）と、第3セキュリティ層（ソフトセキュリティ）と、第4セキュリティ層（データベース多重暗号化）とから成っている。

【0011】

第1セキュリティ層（DBカードセキュリティ）は、携帯端末装置2が任意のDBカードをアクセスする際に、あるいはDBカード3が任意の端末装置によってアクセスされる際において、端末およびカード内にそれぞれ記憶されている第1の識別情報（後述するハード識別番号）同士を照合し、その照合結果に基づいて当該カード自体に対するアクセス可否を決定するチェック処理である。このチェック処理は端末の電源投入時において、カード内に格納されている基本ソフトの起動によって実行開始される。

【0012】

ここで、「ハード識別番号」は、携帯端末装置2とDBカード3とを対応付けておくために予め携帯端末装置2やDBカード3に書き込まれたものである。すなわち、サーバ装置1が携帯端末装置2やDBカード3へ書き込むための内容を予めテーブル設定しておく際に、「ハード識別番号」は、同一グループに属する携帯端末装置2のうち、いずれか一台の端末から読み込んだ固有の端末識別情報（製造番号）に応じて生成されたもので、サーバ装置1はグループ対応の各携帯端末装置2およびそれらの端末で利用される各DBカード3内に、ハード識別番

号をそれぞれ書き込む。したがって、同一グループに属する各携帯端末装置2および各DBカード3内には、それぞれ同一のハード識別番号が共通のアクセス制限情報としてそれぞれ書き込まれる。

【0013】

第2セキュリティ層（パスワード認証）は、上述のDBカードセキュリティチェックの結果、当該カード自体に対するアクセスが許可された場合に、入力されたユーザ認証情報（パスワード）に基づいて正当なオペレータかを照合するチェック処理である。

この場合の照合には、暗号化パスワードが用いられる。すなわち、この暗号化パスワードは、入力されたパスワードを所定の方法で暗号化したもので、端末対応の各DBカード3内にユーザ固有の認証情報としてそれぞれ書き込まれる。この場合、その端末に対してアクセス権限が付与されている複数のユーザが存在している場合には、各ユーザ毎に暗号化パスワードの書き込みが行われる。

【0014】

なお、この第2セキュリティ層においては、DBカード3の利用時において、ユーザパスワードが入力された際に、間違ったパスワードが連続して何回か繰り返して誤入力された場合、その繰り返し入力回数が予め設定されている限度値（後述するビューア不動作設定回数）に達したことが判別されると、それ以降、検索ビューア（パスワード入力を促す表示等の初期画面表示）を不動作とすることにより、パスワード入力を受け付けない状態とするセキュリティ処理も合わせて行うようにしている。

【0015】

第3セキュリティ層（ソフトセキュリティ）は、携帯端末装置2が任意のDBカードをアクセスする際に、あるいはDBカード3が任意の端末装置によってアクセスされる際において、端末およびカード内にそれぞれ記憶されている第2の識別情報（後述するソフト識別番号）同士を照合し、その照合結果に基づいて当該カード内のデータベース（モバイルDB）に対するアクセス可否を決定するチェック処理である。

この「ソフト識別番号」は、DBカード3内のデータベースと、それを利用可

能な携帯端末装置 2 とを対応付けておくために予め携帯端末装置 2 や DB カード 3 に書き込まれたものである。すなわち、サーバ装置 1 が携帯端末装置 2 や DB カード 3 へ書き込むための内容を予めテーブル設定しておく際に、「ソフト識別番号」は、同一グループに属する携帯端末装置 2 のうち、そのいずれか一台の端末から読み込んだ固有の端末識別情報（製造番号）と、そのグループ名称、所定のマスタ DB 名に応じて生成されたもので、サーバ装置 1 はグループ対応の各携帯端末装置 2 およびそれらの端末に対応付けられている各 DB カード 3 内に、ソフト識別番号をそれぞれ書き込む。

【 0 0 1 6 】

第 4 セキュリティ層（データベース多重暗号化）は、DB カードを紛失したり、盗難されたような場合に、仮に、第三者がその DB カードに対してアクセスすることができたとしても、DB カード内のデータベースを多重暗号化によってその解読を防止するセキュリティ対策を示している。

ここで、サーバ装置 1 は DB カード 3 にデータベースを書き込んで配布する際に、配布先のグループに対応付けられているマスタデータベースをそのままカードに書き込むのではなく、マスタデータベースから当該グループの業務内容に応じて必要なデータ内容のみを切り出し、切り出したデータからなるグループ対応のデータベース（モバイル DB）を作成するようにしているが、その際、作成されたモバイル DB のファイル管理情報、つまり、各ファイルの格納位置を示す F A T (F i l e ・ A l l o c a t i o n ・ T a b l e) をスクランブル処理（暗号化処理）するようにしている。

この F A T スクランブル処理は、スクランブル処理用として任意に生成された暗号キー（スクランブルキー）を用いて行われるが、スクランブル処理をどのような手法で行うかは、任意である。

また、サーバ装置 1 は DB カード 3 内にモバイル DB を書き込む際に、任意に生成したレコード暗号化キーを用いて 1 レコード、フィールド毎にモバイル DB の各レコードを個別に暗号化するようにしている。このようにモバイル DB は多重暗号化されて DB カード内に書き込まれる。

【 0 0 1 7 】

図4 (A) は、サーバ装置1側に設けられている設定テーブル11を示している。この設定テーブル11はサーバ装置1がDBカード3や携帯端末装置2に書き込むための各種の内容を予め設定しておくもので、この実施形態においては、DBカード3への書き込みを携帯端末装置2自体に行わせるのではなく、サーバ装置1が一括して行うようにしている。

設定テーブル11はグループ「営業1課」、「営業2課」、「プロジェクトA」、「プロジェクトB」、……のような端末グループ毎に、各種の設定エリアを有する構成となっている。この各グループ毎の設定エリアにセットされた内容は、当該グループ対応の各携帯端末装置2や各DBカード3内に書き込まれる。なお、図4 (A) は、端末グループとして「営業1課」、「営業2課」、「営業1課」を例示した場合を示している。

まず、各グループ対応の設定エリアには「グループ名称」の他、上述した「ハード識別番号」、同一グループに属する端末の合計「設定台数」、その各端末毎の「端末名(1)、端末名(2)、……」、同一グループ内において、その端末を使用することができる権限を持つユーザの合計「使用人数」がそれぞれ設定されている。

【0018】

更に、グループ毎に設定されている「ビューア不動作設定回数(N)」は、パスワードの誤入力が続いて何回か繰り返された場合、それ以降、検索ビューアを不動作とするためにグループ毎に任意に設定された設定回数である。

また、使用の権限を有する各ユーザに対応付けて、その「ユーザ名(1)」、「パスワード」、「ユーザ名(2)」、……が設定されている。また、グループ毎に上述した「スクランブルキー(SK)」、「レコード暗号化キー(RK)」がそれぞれ設定されている。

【0019】

また、書き込み対象としての各データベースに対応付けて、その「モバイルBD名(1)」、「マスタDB名」、「レコード抽出条件」、「抽出対象フィールド」、「モバイルBD名(2)」……が設定されている。

「マスタDB名」は、図4 (B) で示すように、サーバ装置側で記憶管理さ

れている複数のマスタDBファイル12のうち、当該グループの業務内容等に応じて必要とするマスタDBを指定するものであり、また、「レコード抽出条件」、「抽出対象フィールド」は、そのマスタDBを当該グループの業務内容等に応じて修正変更することによってグループ対応のモバイルBDを作成する際に使用されるモバイルBD作成用の条件を定義するものである。

すなわち、「レコード抽出条件」はこのマスタDBから所望するレコード群を抽出するための抽出条件を示し、「抽出対象フィールド」はこの抽出レコード群から所望するフィールドのみからなるレコード構成に変更するためのフィールド抽出条件を示している。そして、「レコード抽出条件」、「抽出対象フィールド」をマスタBD毎に設定しておくことにより、当該グループの業務内容や携帯端末毎の処理内容にマッチした固有のモバイルBDが作成される。

【0020】

また、「モバイルDB名(1)」、「モバイルDB名(2)」……に対応付けて「カスタマイズAP(1)」、「カスタマイズAP(2)」……が設定されている。この「カスタマイズAP」は上述のモバイルBDを処理するためのアプリケーションソフトであり、マスタDB対応の基本AP13(図4(C)参照)をモバイルBDに応じてその表示形態を修正変更したものである。

この「対応カスタマイズAP」には上述した「ソフト識別番号」、「更新日付」、「対応モバイルDB名」が対応設定されている。この場合、「ソフト識別番号」は同一グループ内の各「カスタマイズAP」に共通して設定されるが、「更新日付」はその基本APを修正変更した時の日によって相違する。

なお、「カスタマイズAP」の設定エリアに、そのAP名だけをセットするようにしてもよい。この場合には、当該カスタマイズAP自体は別ファイルに格納しておき、設定テーブル11内の対応カスタマイズAP名に応じて当該アプリケーションソフト自体を呼び出すようにしてもよい。

【0021】

一方、設定テーブル11には、各グループに共通して各DBカードに書き込まれる共通の書き込み対象として、「基本ソフト」がグループ対応設定エリアとは別のエリアに設定されている。ここで、「基本ソフト」には「検索ビューア」

、「FATスクランブル／解除アルゴリズム」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」を含む構成となっている。

「基本ソフト」は、携帯端末装置の基本的な動作を実行制御するための基本ソフトであり、「検索ビューア」は基本ソフトの動作に応じて初期画面（ログイン入力画面）を表示させるソフトである。「動作制御管理ファイル」はDB対応カスタマイズAPを動作制御するための基本的な管理情報が格納されているファイルである。この「動作制御管理ファイル」は通常カード内に書き込まれているが、この実施形態においては、パスワードの誤入力が連続して何回か繰り返された場合、それ以降、検索ビューアを不作動とするために、「動作制御管理ファイル」を削除するようにしており、検索ビューア起動時に、この「動作制御管理ファイル」がDBカード内に存在していることを条件として、携帯端末装置はログイン入力画面を表示させるようにしている。

【0022】

図5は、サーバ装置によって各DBカード3に書き込まれた内容を示している。すなわち、DBカードには、「ハード識別番号」、「FAT（スクランブル済み）」、「基本ソフト」、「検索ビューア」、「FATスクランブル／解除アルゴリズム」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」、「ビューア不作動設定回数」が書き込まれている。「FAT（スクランブル済み）」は当該DBカード内の各モバイルDBを管理する管理情報であり、スクランブル処理された内容のまま書き込まれている。

更に、当該DBカードを使用可能な各ユーザに対応して「ユーザ名（1）」、「暗号化パスワード＋時間変数キー」、「ユーザ名（2）」……が書き込まれていると共に、「レコード暗号化キー（RK）」が書き込まれている。

また、「モバイルDB名（1）」、その実データである「DB（暗号済み）」、「モバイルDB名（2）」……が書き込まれ、更にモバイルDBに対応付けて「カスタマイズAP（1）」と、「ソフト識別番号」、「更新日付」、「対応モバイルDB名」、「カスタマイズAP（2）」……が書き込まれている。

【0023】

図6は、各携帯端末装置2の内蔵メモリに書き込まれた内容を示している。

この内蔵メモリには、図示のようにフラッシュROM、RAM（一時記憶メモリ）が設けられている。このROM、RAMは、セキュリティ対策をも考慮して必要最小限のメモリ容量とした構成となっている。すなわち、この実施形態においては、上述のように、アプリケーション、データベース、基本ソフト等の格納場所を携帯端末装置2とDBカード3とに分散せず、DBカード3にアプリケーション、データベースの他、基本ソフトをも書き込むようにしており、携帯端末自体の紛失、盗難等によるリスクを解消できるようにしている。

ここで、サーバ装置1の書き込み動作によって端末内のフラッシュROMには、上述した「ハード識別番号」、「ソフト識別番号」、「スクランブルキー（SK）」が固定的に記憶される。また、一時記憶メモリであるRAMは、「キー／データ入力エリア」、「FAT読み出しエリア」、「レコードエリア」、「その他のワークエリア」を有する構成となっている。なお、「レコードエリア」は端末内にデータを残さないようにするため、必要最小限のデータ、つまり、現在処理中のカレント分として1レコード分のデータを一時記憶する構成となっている。なお、図示しないが、各携帯端末装置2の内部メモリには、それが製造された端末固有の製造番号も固定的に記憶されている。

【0024】

図7は、サーバ装置1、携帯端末装置2の全体構成を示したブロック図である。

ここで、サーバ装置1、携帯端末装置2の構成要素として基本的に同様なものは、同一番号を付してその説明を兼用するが、サーバ装置1、携帯端末装置2との構成要素を識別するために、サーバ装置1の構成要素には、図中「A」を付し、以下、携帯端末装置2の構成のみを説明し、サーバ装置1の説明は省略するものとする。

CPU21は、記憶装置22内のオペレーティングシステムや各種アプリケーションソフトにしたがってこの携帯端末装置2の全体動作を制御する中央演算処理装置である。記憶装置22は、オペレーティングシステムや各種アプリケーションソフトの他、データベース、文字フォント等が格納され、磁氣的、光学的、半導体メモリ等によって構成されている記録媒体23やその駆動系を有してい

る。この記録媒体23はハードディスク等の固定的な媒体若しくは着脱自在に装着可能なCD-ROM、フロッピーディスク、RAMカード、磁気カード等の可搬型の媒体である。また、この記録媒体23内のプログラムやデータは、必要に応じてCPU21の制御によりRAM（例えば、スタティックRAM）24にロードされたり、RAM24内のデータが記録媒体23にセーブされる。更に、記録媒体はサーバ等の外部機器側に設けられているものであってもよく、CPU21は伝送媒体を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。

また、CPU21は記録媒体23内に格納されるその一部あるいは全部を他の機器側から伝送媒体を介して取り込み、記録媒体23に新規登録あるいは追加登録することもできる。すなわち、コンピュータ通信システムを構成する他の機器から通信回線やケーブル等の有線伝送路あるいは電波、マイクロウェーブ、赤外線等の無線伝送路を介して送信されてきたプログラム／データを伝送制御部25によって受信して記録媒体23内にインストールすることができる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、CPU21は伝送媒体を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。

一方、CPU21にはその入出力周辺デバイスである伝送制御部25、入力部26、表示部27がバスラインを介して接続されており、入出力プログラムにしたがってCPU21はそれらの動作を制御する。入力部26はキーボードやタッチパネルあるいはマウスやタッチ入力ペン等のポインティングデバイスを構成する操作部であり、文字列データや各種コマンドを入力する。

【0025】

次に、この一実施形態におけるセキュリティ管理システムの動作を図8～図11および図13～図17に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記録媒体23（23A）に格納されており、CPU21（21A）はこのプログラムコードにしたがった動作を逐次実行する。また、CPU21（21A）は伝送媒体を介して伝送されてきた上述

のプログラムコードにしたがった動作を逐次実行することもできる。すなわち、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

【0026】

図8および図9は、サーバ装置1が設定テーブル11に対して各種設定を行う場合の動作を示したフローチャートである。

まず、基本的なグループ情報を設定登録する処理が行われる（ステップA1～A10）。ここで、オペレータは入力可能な状態において、今回設定する1グループ分の「グループ名称」を入力指定すると共に（ステップA1）、そのグループ内の端末「設定台数」、ユーザ「使用人数」の入力を行う（ステップA2）。そして、指定台数分の携帯端末装置2と、その端末に対応付けるDBカード3とをサーバ装置1にセットした後（ステップA3）、セットした台数分の「端末名」をそれぞれ入力する（ステップA4）。

【0027】

すると、サーバ装置1はセットされている同一グループ内の各端末のうち、いずれか1台の端末を選択指定して、その「製造番号」を読み出すと共に（ステップA5）、この「製造番号」に基づいて「ハード識別番号」を生成して（ステップA6）、設定台数分の各携帯端末装置2およびDBカード3に「ハード識別番号」をそれぞれ書き込む（ステップA7）。なお、テーブル設定時において、携帯端末装置／DBカードへの書き込みは、「ハード識別番号」の生成時と後述する「ソフト識別番号」生成時および「スクランブルキー（SK）」の生成時の場合に限りに行うようにしている。

次のステップA8では、上述のように入力された「グループ名称」、「設定台数」、「端末名」、「使用人数」の他、生成した「ハード識別番号」を設定テーブル11にそれぞれ登録する処理が行われる。

そして、パスワード不一致でのビューア不作動回数として任意の値をオペレータが入力すると（ステップA9）、入力された「ビューア不作動回数」は、設定テーブル11に登録される（ステップA10）。

【0028】

このようにしてグループ基本情報の設定登録が終わると、そのグループの使用人数分のパスワードを設定登録する処理に移る（ステップA11～A15）。

まず、オペレータはユーザ名を入力すると共に（ステップA1）、そのユーザ対応のパスワードを入力すると（ステップA12）、入力されたユーザ名、パスワードは設定テーブル11にそれぞれ登録される（ステップA13）。これによって一人分のユーザ登録が終わると、使用人数分のユーザ登録が終了したかを調べ（ステップA14）、全ユーザ分の設定が終了するまで上述の動作を繰り返す。

【0029】

そして、ユーザ登録が終了すると、次に、「スクランブルキー（SK）」、「レコード暗号化キー（RK）」を設定登録する処理に移る（ステップA15～A17）。

まず、「スクランブルキー（SK）」を生成すると共に（ステップA15）、「レコード暗号化キー（RK）」を生成する（ステップA16）。この「スクランブルキー（SK）」は上述したように、モバイルDBのFATをスクランブル処理する際に使用される暗号キーであり、また、「レコード暗号化キー（RK）」は、データベースを1レコード、フィールド毎に暗号化する際に使用される暗号化キーである。この場合のキー生成方法は、任意であり、その都度、ランダムに生成するようにしてもよい。

そして、生成した「スクランブルキー（SK）」、「レコード暗号化キー（RK）」を設定テーブル11にそれぞれ登録すると共に（ステップA17）、生成した「スクランブルキー（SK）」を設定台数分、各携帯端末装置2にそれぞれ書き込む（ステップA18）。

【0030】

次に、データベースおよびそれに対応するアプリケーションソフトを設定登録する処理に移る（図9のステップA20～A34）。

まず、オペレータはDBカードに書き込むための「モバイルDB名」およびその作成の元となる「マスタDB名」を指定入力すると（ステップA20、A21）、この「モバイルDB名」と共に「マスタDB名」は、設定テーブル11に対

応して登録される（ステップA22）。そして、指定されたマスタDBにおけるファイルのレコード構成が案内表示される（ステップA23）。すなわち、マスタDBの各レコードが図12（A）に示すように8フィールド「A」、「B」～「H」の各項目から構成されているものとする、この1レコード分の各項目名がその並び順に案内表示される。

【0031】

ここで、オペレータはレコード構成の案内表示を確認し、「レコード抽出条件」を指定入力する（ステップA24）。つまり、案内表示されているレコード構成の各フィールドうち、所望するフィールドを条件設定対象フィールドとして指定した後、その指定フィールドに対する「レコード抽出条件」を指定入力する。例えば、更新日付の項目を条件設定対象フィールドとして指定した後、1999年12月24日以降に更新されたレコードを「レコード抽出条件」として指定する。次に、レコード構成の対象とするフィールドを選択指定する（ステップA25）。例えば、案内表示されているレコード構成の各フィールドうち、所望するフィールドを「抽出対象フィールド」として選択指定する。すると、指定入力された「レコード抽出条件」およびレコード構成の「対象フィールド名」が当該モバイルDB名に対応して設定テーブル11にそれぞれ登録される（ステップA26）。

そして、当該グループで使用する書き込み対象としての全てのモバイルDBを指定し終わったかを調べ（ステップA27）、全ての指定が終わるまで、上述の動作を繰り返すことにより、モバイルDBの設定登録を行う（ステップA20～A27）。

【0032】

これによって、モバイルDBの設定登録が終わると、上述のようにして読み込んだ「製造番号」と、当該グループ内において最初に指定された「モバイルDB名」と、入力された「グループ名」とに基づいて「ソフト識別番号」を生成すると共に（ステップA28）、この「ソフト識別番号」を設定台数分の携帯端末装置2にそれぞれ書き込む（ステップA29）。

次に、今回設定登録した各モバイルDB名に対応付けてそのカスタマイズAP

を設定登録する処理に移る。すなわち、設定登録した各モバイルDB名のうち、そのいずれかをオペレータが指定すると（ステップA30）、指定されたモバイルDB名に対応する「マスタDB名」が読み出され、このマスタDB対応の基本AP13をアクセスし、当該モバイルDBを利用するための表示形態に、この基本APを修正変更することにより、所望するカスタマイズAPを任意に作成する（ステップA31）。

【0033】

例えば、当該モバイルDBのレコード構成に応じてどのフィールドをどの位置に表示させるかを指定したり、各フィールドの表示サイズ等を任意に指定しながら基本APを修正変更することにより、所望するカスタマイズAPを作成する。

そして、作成したカスタマイズAPに「ソフト識別番号」、現在のシステム日付である「更新日付」、「対応モバイルDB名」を書き込んだ後（ステップA32）、このカスタマイズAPを設定テーブル11に登録する（ステップA33）。そして、全てのカスタマイズAPを作成登録し終わるまで（ステップA34）、上述の動作を繰り返す（ステップA30～A34）。

【0034】

次に、全てのグループに対する設定登録が終了したかを調べ（ステップA35）、全グループ終了が判別されるまでステップA1に戻り、1グループ毎に上述の動作を繰り返す。これによって設定テーブル11には、各グループに対応して図4に示した各種の内容が設定登録される。その際、1グループ分の設定登録が終了する毎に、次の設定対象グループを指定して、そのグループ対応の携帯端末装置2、DBカード3をサーバ装置1にセットする。このようなテーブル設定によって携帯端末装置2には「ハード識別番号」、「ソフト識別番号」、「スクランブルキー（SK）」がそれぞれ書き込まれ、更に、DBカード3には「ハード識別番号」、「ソフト識別番号」がそれぞれ書き込まれる。

【0035】

図10および図11は、サーバ装置1がモバイルDBや対応カスタマイズAP等をDBカード3に書き込んで配布する場合の動作を示したフローチャートである。

先ず、オペレータはサーバ装置1に配布対象の1または2以上のDBカード3をセットする(ステップB1)。すると、セットされているDBカードの中から1つのカードを選択して、そのカード内から「ハード識別番号」を読み出すと共に(ステップB2)、このハード識別番号に基づいて設定テーブル11を検索し、該当するグループを特定しておく(ステップB3)。

そして、各グループに共通して各DBカードに書き込まれる共通の書き込み対象としての「基本ソフト」を設定テーブル11から読み出し、そのDBカードに書き込む(ステップB4)。この場合、「基本ソフト」には「検索ビューア」、「FATスクランブル/解除アルゴリズム」、「暗号化/復号化アルゴリズム」、「動作制御管理ファイル」が含まれているので、それらを含めて書き込まれる。

次に、特定したグループ対応の「ビューア不作動設定回数(N)」を設定テーブル11から読み出してDBカードに書き込む(ステップB5)。

【0036】

更に、現在のシステム日時を取得し、これを時間変数キーとして特定しておく(ステップB6)。そして、特定グループの各ユーザのうち、その先頭のユーザから対応する「パスワード」を読み出し(ステップB7)、上述の時間変数をキーとして、この「パスワード」を暗号化する(ステップB8)。これによって生成された暗号化パスワードに「時間変数キー」を付加して、対応するユーザ名と共にDBカードに書き込む(ステップB9)。

そして、特定グループの各ユーザを全て指定し終わったかを調べ(ステップB10)、全て指定し終わるまでステップB7に戻り、上述の動作を各ユーザ毎に繰り返す。これによって全ユーザ分の処理が終了すると、設定テーブル11から特定グループの「レコード暗号化キー(RK)」を読み出してDBカードに書き込む(ステップB11)。

【0037】

次に、モバイルDB作成してDBカードに書き込む処理に移る。

先ず、設定テーブル11に登録されている特定グループ対応の各モバイルDB名のうち、その先頭のモバイルDB名に対応づけられているマスタDB名に該当

するマスタDBファイルを読み出しておく（ステップB12）。そして、このマスタDB名対応の「レコード抽出条件」、「抽出対象フィールド」をそれぞれ取得し、この「レコード抽出条件」に基づいてマスタDBファイル12を検索することにより該当レコードを抽出する（ステップB13）。すなわち、図12（B）は、この場合の具体例を示し、マスタDB（図12（A）参照）から「レコード抽出条件」に該当する各レコード群を切り出すことによって、当該グループの業務内容や端末の処理内容に必要なレコード群のみが抽出される。

【0038】

これによって抽出した各レコード群を「抽出対象フィールド」に基づいて、そのレコード構成を変更する（ステップB14）。図13（C）は、この場合の具体例を示し、抽出されたレコード群は、それを構成する各フィールドのうち、「抽出対象フィールド」に該当するフィールドのみが切り出され、切り出されたフィールドのみからなるレコード構成に変更される。

次に、図11のステップB15に移り、上述のようにレコード構成を変更した後の各レコード・フィールドを「レコード暗号化キー（RK）」に基づいて暗号化する。この場合、各レコード・フィールドを暗号化する毎に、「レコード暗号化キー（RK）」の値を更新することによって、それぞれ異なるキーを用いて個別に暗号化するようにしている。そして、暗号化したレコード群をモバイルDBファイルとして作成して、DBカードに書き込む（ステップB16）。

このようにして1ファイル分のモバイルDBを作成すると、特定グループに対応して他のモバイルDB名が設定登録されているかを調べ（ステップB17）、有れば、ステップB12に戻り、上述の動作を繰り返す。

これによって、特定グループ対応の各モバイルDB名毎に、モバイルDBファイルが作成されてDBカード内に書き込まれると共に、そのファイルの格納位置を示すFATが作成されてDBカード内に書き込まれる。

【0039】

次に、モバイルDB対応のカスタマイズAPをDBカードに書き込む処理に移る。まず、マスタDB名に基づいてそれに対応付けられているカスタマイズAPを設定テーブル11から読み出し（ステップB18）、それに対応カスタマイズ

APがDBカード内に存在しているかを調べるが（ステップB20）、最初は存在していないので、ステップB24に進み、設定テーブル11内の現行のカスタマイズAPを読み出してDBカードに上書きする。これによってDBカード内には、モバイルDBに対応して最新のカスタマイズAP（「ソフト識別番号」、「更新日付」を含む）が新規に書き込まれる

【0040】

また、DBカード内にカスタマイズAPは存在している場合であっても（ステップB19）、そのDBカード内の「更新日付」と、現行のカスタマイズAPの「更新日付」とを比較し、両者の不一致が判別された場合（ステップB20）、つまり、現行のカスタマイズAPが更新されている場合にも、ステップB24に進み、現行のカスタマイズAPをDBカードに上書きすることによって最新のカスタマイズAPに書き換えられる。なお、「更新日付」が一致する場合には、DBカード内のカスタマイズAPは最新のものであるため、その更新は行われない。

そして、同一グループ内に他のカスタマイズAPが設定されているかを調べ（ステップB21）、有れば、ステップB18に戻り、次のカスタマイズAPを読み出し、以下同様の処理を繰り返す。

そして、カスタマイズAPの書き込みが終わると、DBカード内のモバイルDBの各ファイル格納位置を示すFATを「スクランブルキー（SK）」を用いてスクランブル化する（ステップB22）。

【0041】

これによってDBカード1枚分の書き込み処理が終わると、未書き込みのDBカードが他に有るかを判別し（ステップB23）、他のDBカードがセットされていれば、図10のステップB2に戻り、未書き込みのDBカードの中からその1つを指定して上述の動作を繰り返す。これによってサーバ装置にセットされている各DBカードには、図6に示した内容がそれぞれ書き込まれる。

このようにして基本ソフト、ユーザ情報、モバイルDB、対応カスタマイズAP等が書き込まれたDBカードは、グループ毎に当該ユーザに配布される。

【0042】

図13は、携帯端末装置側において電源投入に応じて実行開始されるフローチャートである。

まず、携帯端末装置にDBカードがセットされている状態において、電源がオンされると、DBカード内の基本ソフトに基づいて基本動作が開始される（ステップC1）。すると、上述した第1セキュリティ層のDBカードセキュリティ処理が実行される。すなわち、DBカードから「ハード識別番号」を読み出し（ステップC2）、当該端末内の「ハード識別番号」と照合する（ステップC3）。この結果、両者が一致する場合には（ステップC4）、当該端末とカードとは正当な対応関係にあるので、DBカード内のスクランブル済み「FAT」を端末側に読み込み、これを図6で示したRAM内の「FAT読み出しエリア」にセットし（ステップC5）、この「FAT」を端末内の「スクランブルキー（SK）」を用いてそのスクランブルを解除する（ステップC6）。そして、検索ビューアを起動させる（ステップC7）。

また、当該端末とカードとが正当な対応関係にない場合には、「ハード識別番号」の不一致が判別されるので、ハードエラー表示を行った後（ステップC8）、電源を強制的にオフし（ステップC9）、エラー終了となる。

【0043】

図14は、図13のステップC7（検索ビューア起動）時の動作を詳述するためのフローチャートである。

まず、上述した第2セキュリティ層のパスワード認証処理において、その前段階としてのセキュリティ処理が実行される。すなわち、携帯端末装置は検索ビューア起動時にDBカードをアクセスし、カード内に「動作制御管理ファイル」が存在しているかをチェックする（ステップD1）。ここで、上述したように、パスワードの誤入力が続いて何回か繰り返された場合、それ以降、検索ビューアを不作動とするために、「動作制御管理ファイル」を削除するようにしている。したがって、「動作制御管理ファイル」の存在有無をチェックし、それが存在していなければ、不作動メッセージを表示させた後（ステップD11）、電源を強制的にオフして（ステップD11）、エラー終了となる。

【0044】

一方、「動作制御管理ファイル」が存在していれば、それを条件としてログイン入力画面を表示させてユーザ名、パスワード入力を促すメッセージを表示する（ステップD2）。ここで、オペレータが自己の「ユーザ名」、「パスワード」を入力すると（ステップD3）、DBカード内の「ユーザ名」対応の暗号化パスワードを読み出し（ステップD4）、この暗号化パスワードを「時間変数」をキーとして復号化する（ステップD5）。そして、入力されたパスワードと復号化されたパスワードとを照合する（ステップD6）。

その結果、両者の不一致が判別された場合には（ステップD7）、その不一致回数を更新すると共に、その更新値と、予めグループ毎に設定されている「ビューア不作動設定回数（N）」とを比較し、パスワードの誤入力が連続してN回繰り返されたかをチェックし（ステップD8）、N回未満であれば、ログイン入力画面に戻り（ステップD2）、その再入力を受け付ける。

いま、パスワードの誤入力が連続してN回繰り返されたことが判別された場合には（ステップD8）、「動作制御管理ファイル」を削除すると共に（ステップD9）、不作動メッセージを表示させた後（ステップD10）、電源を強制的にオフして（ステップD11）、エラー終了となる。

【0045】

また、パスワードの誤入力が連続してN回繰り返される前において、パスワードが一致し、正当のオペレータであることが判別された場合には（ステップD7）、先ず、上述した第3セキュリティ層のソフトセキュリティ処理が行われる。すなわち、DBカード内に書き込まれている各カスタマイズAPのメニュー画面が一覧表示されるので、このメニュー画面の中からオペレータが所望するカスタマイズAPを選択指定すると（ステップD12）、選択されたカスタマイズAPに含まれている「ソフト識別番号」をDBカード内から読み出し（ステップD13）、自己の端末内の「ソフト識別番号」と照合する（ステップD14）。その結果、両者の不一致が判別された場合には（ステップD15）、不作動メッセージ表示を行うと共に（ステップD10）、電源を強制的にオフして（ステップD11）、エラー終了となる。

一方、「ソフト識別番号」を照合した結果、両者の一致が判別された場合には

、選択されたカスタマイズAPを立ち上げ、それに応じたアプリケーション処理を実行開始させる（ステップD16）。

【0046】

図15および図16は、図14のステップD16（カスタマイズAP起動）時の動作を詳述するためのフローチャートである。

まず、処理メニュー表示が行われる（ステップE1）。この場合のメニュー画面には「キー検索」、「追加」、「終了」の各メニュー項目が表示され、その中から所望するメニュー項目を選択指定すると（ステップE2）、選択項目を調べ（ステップE3、E13）それにに応じた処理に移る。

【0047】

ここで、メニュー項目「キー検索」が選択された場合において、検索キー（例えば、商品名や得意先名等）が入力されると（ステップE4）、DBカードから「レコード暗号化キー」を読み込み、この検索キーを「レコード暗号化キー（RK）」で暗号化する（ステップE5）。そして、DBカード内のモバイルDBを暗号化された検索キーを用いて検索して（ステップE6）、そのキーに該当するレコードを抽出するが、一致するキーが無ければ（ステップE7）、メニュー表示画面に戻り（ステップE1）、検索キーの再入力が可能となる。

いま、キー検索の結果、一致するキーが有れば（ステップE7）、ステップE8に移り、当該モバイルDBから検索キーに該当するレコードを読み出して、図6で示したRAM内の「レコードエリア」に書き込む。そして、このレコードを「レコード暗号化キー（RK）」で復号化して（ステップE9）、そのレコード内容を表示出力させると共に（ステップE10）、処理メニュー表示が行われる（ステップE11）。

【0048】

この場合のメニュー画面には「訂正」、「削除」、「終了」の各メニュー項目が表示されるので、その中から所望するメニュー項目を選択指定する（ステップE12）。すると、選択項目を調べ（図16のステップE20、E26）それにに応じた処理に移る。

すなわち、メニュー項目「訂正」が選択された場合において（ステップE20）

、訂正データが入力されると、それに応じてレコード内容を訂正する処理が行われる（ステップE 2 1）。そして、レコード訂正が行われたことを示すために、その訂正レコードに「訂正フラグ」をセットすると共に（ステップE 2 2）、訂正レコードを「レコード暗号化キー（RK）」を用いて暗号化し（ステップE 2 3）、この暗号化レコードを当該モバイルDB内の元のレコードに上書きする（ステップE 2 4）。

これによってレコード訂正が終了すると、その端末内から当該レコードを削除しておく（ステップE 2 5）。つまり、図6で示したRAM内の「レコードエリア」をクリアする。

また、メニュー項目「削除」が選択された場合には（ステップE 2 6）、該当レコードのデータ部を削除し、そのレコードに「削除フラグ」をセットして、当該モバイルDB内の元のレコードに上書きする（ステップE 2 7）。そして、端末内から当該レコードを削除しておく（ステップE 2 5）。

【0049】

他方、図15のステップE 1での処理メニュー画面において、「追加」が選択された場合には、ステップE 1 4に移り、新規レコードの入力作成処理が行われる。そして、レコード追加であることを示すために、新規レコードに「追加フラグ」をセットすると共に（ステップE 1 5）、新規レコードを「レコード暗号化キー（RK）」を用いて暗号化し（ステップE 1 6）、この暗号化レコードを当該モバイルDB内に追加する（ステップE 1 7）。

これによってレコード追加が終了すると、その端末内から当該レコードを削除しておく（図16のステップE 2 5）。

なお、図16のステップE 1での処理メニュー画面において、「終了」が選択された場合には、端末内の「FAT」を削除する（ステップE 1 8）。つまり、図6で示したRAM内の「FAT読み出しエリア」の内容をクリアする。そして、その端末内のレコードを削除する（ステップE 2 5）。

このようにして、携帯端末装置側では、DBカードに格納されているモバイルDBのファイル内容が日常業務の遂行に応じて更新される。

【0050】

図 1 7 は、サーバ装置において、日常業務の遂行に応じて変更された DB カード内のモバイル DB を収集してサーバ内のマスタ DB を更新する場合の動作（回収動作）を示したフローチャートである。

まず、オペレータが回収対象の DB カードをサーバ装置にセットすると（ステップ F 1）、この DB カードから「ハード識別番号」を読み出し（ステップ F 2）、この「ハード識別番号」に基づいて設定テーブル 1 1 を参照し、それに該当するグループを特定する（ステップ F 3）。そして、DB カードから「スクランブルキー（SK）」を読み出し、DB カード内の FAT を「スクランブルキー（SK）」を用いてスクランブル解除する（ステップ F 4）。

また、DB カードからモバイル DB を読み出し（ステップ F 5）、この DB ファイルの各レコード・フィールドを「レコード暗号化キー（RK）」を用いて復号化する（ステップ F 6）。この場合においても、各レコード・フィールドを復号化する毎に、「レコード暗号化キー（RK）」の値を更新することによって、それぞれ異なるキーを用いて復号化を行うようにしている。

【 0 0 5 1 】

そして、復号化した DB ファイル内に変更レコードが存在するかを「訂正フラグ」、「削除フラグ」、「追加フラグ」の有無に基づいて調べ（ステップ F 7）、変更レコードが有れば、つまり、いずれかの「フラグ」が付加されているレコードが存在していれば、そのモバイル DB に対応するサーバ装置内のマスタ DB を特定し（ステップ F 8）、当該モバイル DB から読み出した変更レコードをそれに付加されている「フラグ」の種類に応じてマスタ DB 内の該当レコードを更新する処理を行う（ステップ F 9、F 1 0）。

すなわち、該当するレコード内容を訂正する訂正処理、該当レコードのデータを削除する削除処理、新規レコードを追加する追加処理を行う。このようなマスタ DB のレコード更新処理は、モバイル DB 内の全ての変更レコードに対して行われる（ステップ F 9～F 1 1）。そして、他のモバイル DB が DB カード内に有れば（ステップ F 1 2）、そのモバイル DB に対して上述の動作を繰り返す（ステップ F 5～F 1 2）。

【 0 0 5 2 】

以上のように、この一実施形態においては、携帯端末装置がDBカードをアクセスする際、このカード内の「ハード識別番号」と自己の「ハード識別番号」とを照合し、その照合結果に基づいて当該DBカードに対するアクセス可否を決定し、その結果、当該カードに対するアクセスが許可された際に、このカードに記憶されている「ソフト識別番号」と自己の「ソフト識別番号」とを照合し、その照合結果に基づいて当該カード内のモバイルDBへのアクセス可否を決定するようにしたから、端末と媒体との対応付けにより、そのモバイルDBに対するアクセスの他、このカード自体に対するアクセスをも不可能とする多重セキュリティという万全な対策を講じることができる。

【0053】

これによって、紛失、盗難、悪意等によってDBカード内のモバイルDBが他人に漏洩されることを確実に防止することができる。また、セキュリティ管理のために特別な操作を要求せず、操作性を損なわないセキュリティ管理を実現することができる。すなわち、DBカードを携帯端末装置に装着するだけで自動的にセキュリティ管理が実行されるので、DBカード利用時にユーザはセキュリティ対策を全く意識しなくてもよく、使い勝手を損なわず、確実なセキュリティ管理を実現することができる。

この場合、重要情報を含んだモバイルDBを携帯端末から分離可能なDBカードだけに保管しておくようにしたから、携帯端末のみを紛失したり、盗難されたとしてもセキュリティ上全く問題は無く、また、DBカードを紛失したり、盗難された場合でも、そのカードへのアクセスは、正当の端末しかできないようにした仕組みを持っているため、モバイルDBに対するアクセスはおろか、DBカード自体に対するアクセスをも不可能となり、そのセキュリティは極めて高いものとなる。

【0054】

また、DBカードへのデータファイルの書き込みの他、DBカードとそれをアクセス可能な携帯端末装置との対応付けをサーバ装置が一括して行うことによって、その設定作業を効率よく行うことができると共に、DBカードに対するセキュリティ管理を確実なものとするために、その対策を講じるための仕組みを携帯

端末装置自体に持たる必要がなくなる。また、元となるマスタDBをそのまま書き込むのではなく、マスタDBから切り出したレコード群のみからなるモバイルDBを作成して書き込むことで、当該カード対応の正当な端末に対しても必要以上の情報を提供しないという対策を講じることができる。したがって、元となるマスタDBをそのままカードに書き込む方法では、当該マスタDBに対してレコード毎、フィールド毎にそのアクセスを制限するためのアクセス権限情報を予め設定しておく必要があるが、マスタDBから切り出したレコード群のみからなるモバイルDBを書き込むことにより、アクセス権限情報の設定は一切不用となる。つまり、アクセス権限情報の設定という論理的なセキュリティ対策ではなく、物理的なセキュリティ対策を講じることにより、紛失、盗難、悪意等によるカード内の重要情報の漏洩防止も確実なものとなると共に、記憶容量の点でも有利なものとなる。

【0055】

この場合、携帯端末装置にて利用されるレコード群をマスタDBから切り出す際に、その携帯端末装置側での処理内容に合わせて予め設定されているレコード抽出条件を参照し、このレコード抽出条件に合致するレコード群を切り出すことができると共に、抽出対象フィールドを参照し、この抽出対象フィールドの条件に合致するフィールドのみからなるレコード構成のモバイルDBを作成することができるので、レコード抽出条件、抽出対象フィールドを設定しておくだけで、所望するモバイルDBを容易に作成することができる。また、携帯端末装置にて利用されるレコード群をマスタDBから切り出す際に、書き込み対象のDBカード内に設定されているハード識別情報を取得し、このハード識別情報に基づいて所望するマスタDBを自動決定することが可能となる。

【0056】

また、モバイルDBを処理するためのカスタマイズAPが当該モバイルDBに対応付けてDBカード内に記憶されていない場合には、そのモバイルDBに対応付けてそれを処理するためのカスタマイズAPをDBカード内に書き込み、また、カスタマイズAPがDBカード内に記憶されていても、それが最新のものない場合には、最新のカスタマイズAPに書き換えるようにしたから、DBカード内

にモバイルDBとカスタマイズAPとを対応付けて記憶させることができると共に、最新のカスタマイズAPを常時記憶させることができる。

【0057】

なお、「ハード識別番号」、「ソフト識別番号」をどのような情報に基づいて生成するかは任意であり、例えば、「ハード識別番号」をその携帯端末装置の「製造会社コード」+「製造番号」等で構成してもよい。また、同一DBカード内に複数のモバイルDBが格納されている場合に、各モバイルDB毎に「ソフト識別番号」を相違させてもよい。

また、端末グループは、複数の端末を単に区分けする以外に、1台の端末が複数のグループに属するような設定も可能である。

また、レコード抽出条件、抽出対象フィールドの設定内容を必要に応じて任意に変更するようにしてもよい。更に、最新のカスタマイズAPへ書き換える場合に、その更新日に基づいて最新かを判別するようにしたが、その「バージョンNo.」に基づいてその判別を行うようにしてもよい。

【0058】

また、上述した一実施形態においては、可搬型記憶媒体であるDBカードとして、コンパクトフラッシュカードを例示したが、その他にPCカード、スマートメディア、CD（光ディスク）、MO（光磁気ディスク）、FD（フロッピーディスク）等であってもよく、しかも、カード型に限らず、カセット型、スティック型等、その形状は任意である。

更に、携帯端末装置としては、電子手帳、ノート型パソコン、PDA、携帯電話等であってもよい。

【0059】

【発明の効果】

この発明によれば、可搬型データ記憶媒体に対するセキュリティ管理を確実なものとするために、データ記憶媒体へのデータファイルの書き込みの他、データ記憶媒体とそれをアクセス可能な携帯端末装置との対応付けをサーバ装置が一括して行うことができると共に、元となるマスタデータベースをそのまま書き込むのではなく、マスタデータベースから切り出したレコード群のみからなるモバ

イルデータファイルを作成して書き込むことで、当該媒体対応の正当な端末に対しても必要以上の情報を提供しないという対策を講じることができ、また、紛失、盗難、悪意等によるデータ記憶媒体内の重要情報の漏洩を確実に防止することができる。

【図面の簡単な説明】

【図 1】

セキュリティ管理システムの全体構成を示したブロック図。

【図 2】

端末グループ対応のDBカード3を説明すると共に、携帯端末装置とユーザとの対応関係を説明するための図。

【図 3】

多重セキュリティを概念的に示した図。

【図 4】

(A) は、サーバ装置側に設けられている設定テーブル11の構成とその設定内容を示した図、(B) はマスタDBファイル12を示した図、(C) はDB対応基本AP13を示した図。

【図 5】

各DBカード3に書き込まれた内容を示した図。

【図 6】

各携帯端末装置2の内蔵メモリに書き込まれた内容を示した図。

【図 7】

サーバ装置1、携帯端末装置2の全体構成を示したブロック図。

【図 8】

サーバ装置1が設定テーブル11に対して設定を行う場合の動作を示したフローチャート。

【図 9】

図8に続く設定動作を示したフローチャート。

【図 10】

サーバ装置1がマスタDBやカスタマイズAP等をDBカード3に書き込んで

配布する場合の動作を示したフローチャート。

【図11】

図10に続く配布動作を示したフローチャート。

【図12】

(A) はマスタDBを示した図、(B) はマスタDBから「レコード抽出条件」によって抽出されたレコードを示した図、(C) は各抽出レコードから「抽出対象フィールド」によって変更された変更後のレコード構成を示した図。

【図13】

携帯端末装置2側において電源投入に応じて実行開始されるフローチャート。

【図14】

図13のステップC7（検索ビュー起動）時の動作を詳述するためのフローチャート。

【図15】

図14のステップD16（DB対応のカスタマイズAP起動）時の動作を詳述するためのフローチャート。

【図16】

図15に続くカスタマイズAP起動時の動作を詳述したフローチャート。

【図17】

サーバ装置1において、日常業務の遂行に応じて変更されたDBカード内のモバイルDBを収集してサーバ内のマスタDBを更新する場合の回収動作を示したフローチャート。

【符号の説明】

- 1 サーバ装置
- 2 携帯端末装置
- 3 DBカード
 - 11 設定テーブル
 - 12 マスタDBファイル
 - 13 DB対応基本AP
- 21、21A CPU

2 2、2 2 A 記 憶 装 置

2 3、2 3 A 記 録 媒 体

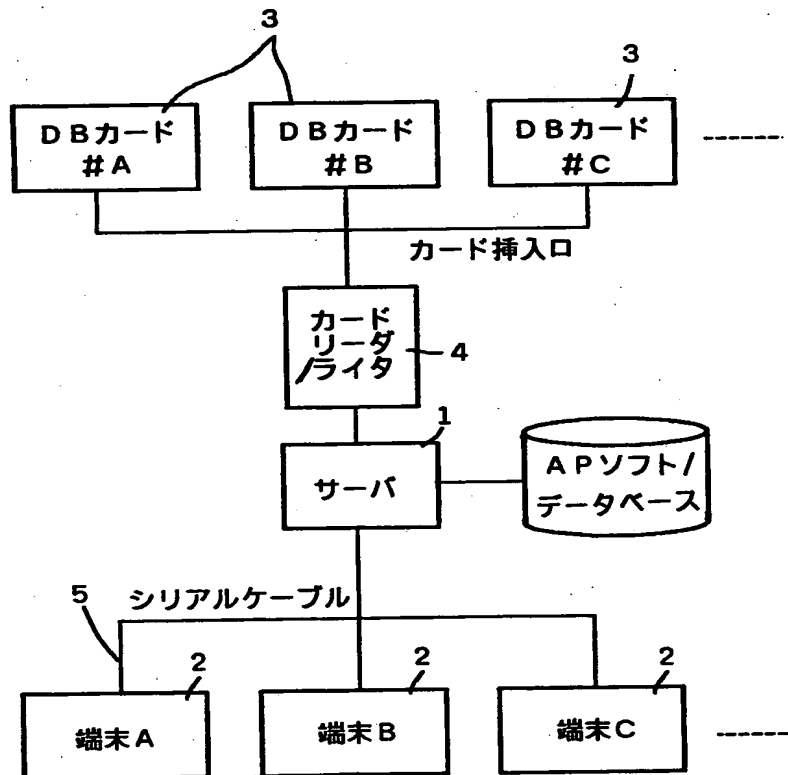
2 5、2 5 A 伝 送 制 御 部

2 6、2 6 A 入 力 部

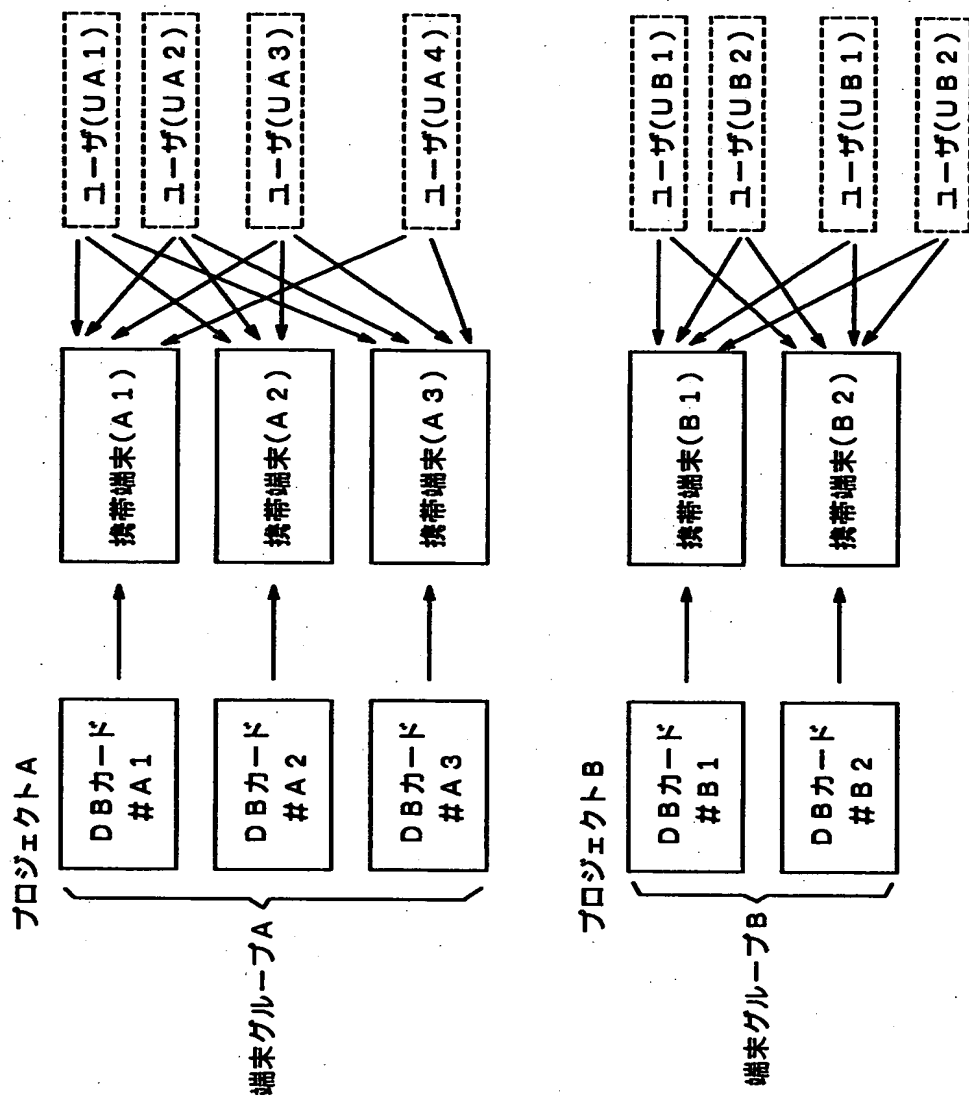
2 7、2 7 A 表 示 部

【書類名】 図面

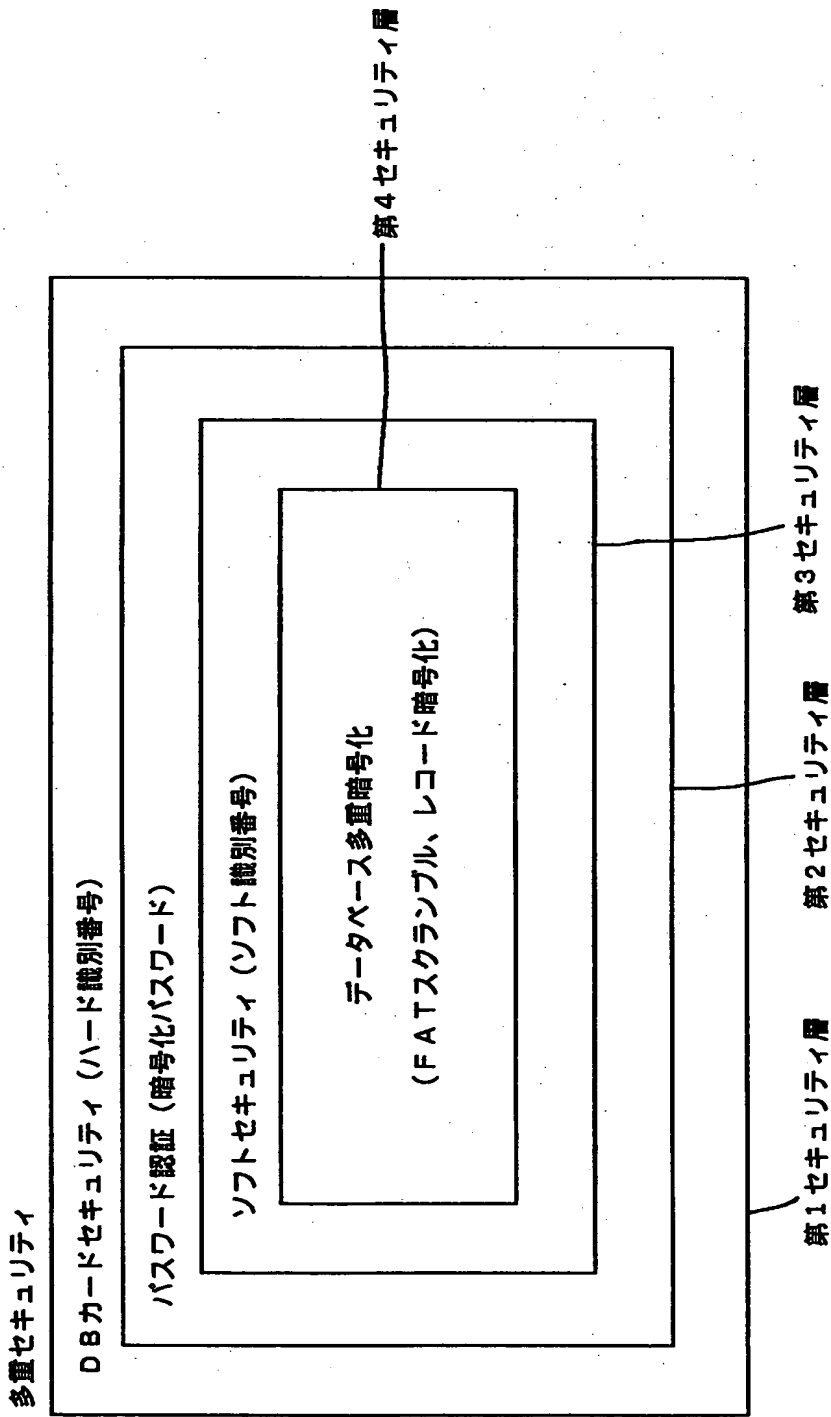
【図1】



【図 2】



【図 3】



【図 4】

サーバ

設定テーブル		グループ	グループ	グループ
グループ名称		営業1課	営業2課	営業3課
ハード識別番号				
設定台数				
端末名(1)				
端末名(2)				
端末名(3)				
使用人数				
ビューア不動作設定回数(N)				
ユーザ名(1)				
パスワード				
ユーザ名(2)				
パスワード				
ユーザ名(3)				
パスワード				
ユーザ名(4)				
パスワード				
スクランブルキー(SK)				
レコード暗号化キー(RK)				
モバイルDB名(1)				
マスタDB名				
レコード抽出条件				
抽出対象フィールド				
モバイルDB名(2)				
マスタDB名				
レコード抽出条件				
抽出対象フィールド				
カスタマイズAP(アプリケーション)(1)				
ソフト識別番号(共通)				
更新日付				
対応モバイルDB名				
カスタマイズAP(アプリケーション)(2)				
ソフト識別番号(共通)				
更新日付				
対応モバイルDB名				
基本ソフト				
検索ビューア				
FATスクランブル/解除アルゴリズム				
暗号化/復合化アルゴリズム				
動作制御管理ファイル				

(A)

11

(B) マスタDBファイル (複数)

(C) マスタDB対応の基本AP (複数)

13

12

【図5】

カード内部構成

ハード識別番号(固定)
FAT(スクランブル済)
基本ソフト
検索ビューア
FATスクランブル/解除アルゴリズム
暗号化/復合化アルゴリズム
動作制御管理ファイル
ビューア不動作設定回数(N)
ユーザ名(1)
暗号化パスワード+時間変数キー
ユーザ名(2)
暗号化パスワード+時間変数キー
ユーザ名(3)
暗号化パスワード+時間変数キー
ユーザ名(4)
暗号化パスワード+時間変数キー
レコード暗号化キー(RK)
モバイルDB名(1)
DB(暗号済)
モバイルDB名(1)
DB(暗号済)
カスタマイズAP(1)
ソフト識別番号(共通)
更新日付
対応モバイルDB名
カスタマイズAP(2)
ソフト識別番号(共通)
更新日付
対応モバイルDB名

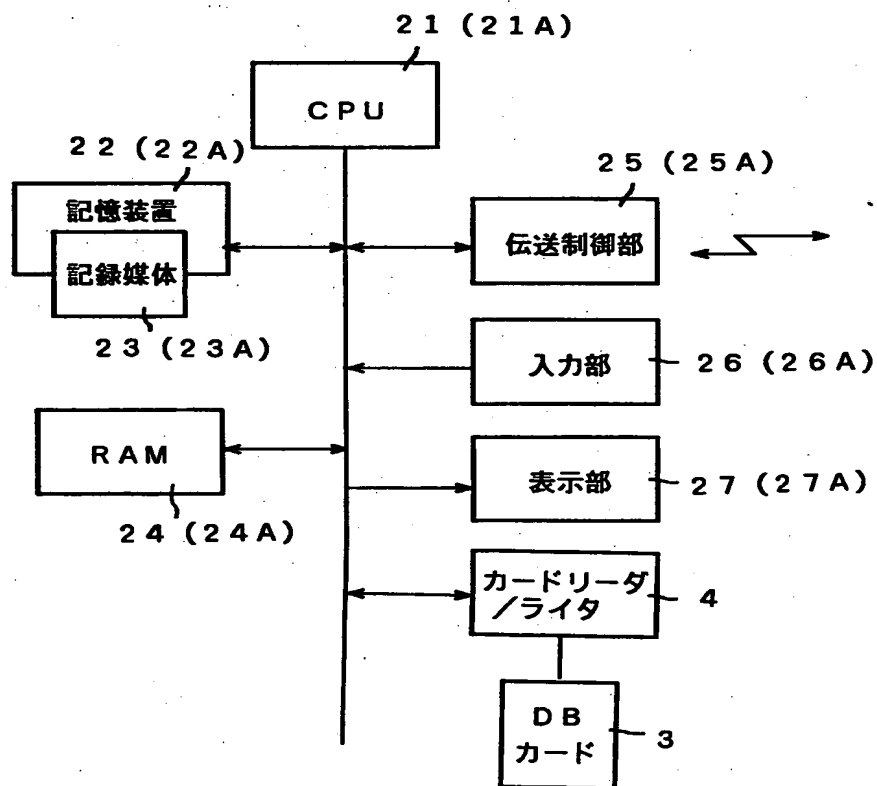
【図 6】

内蔵メモリ構成

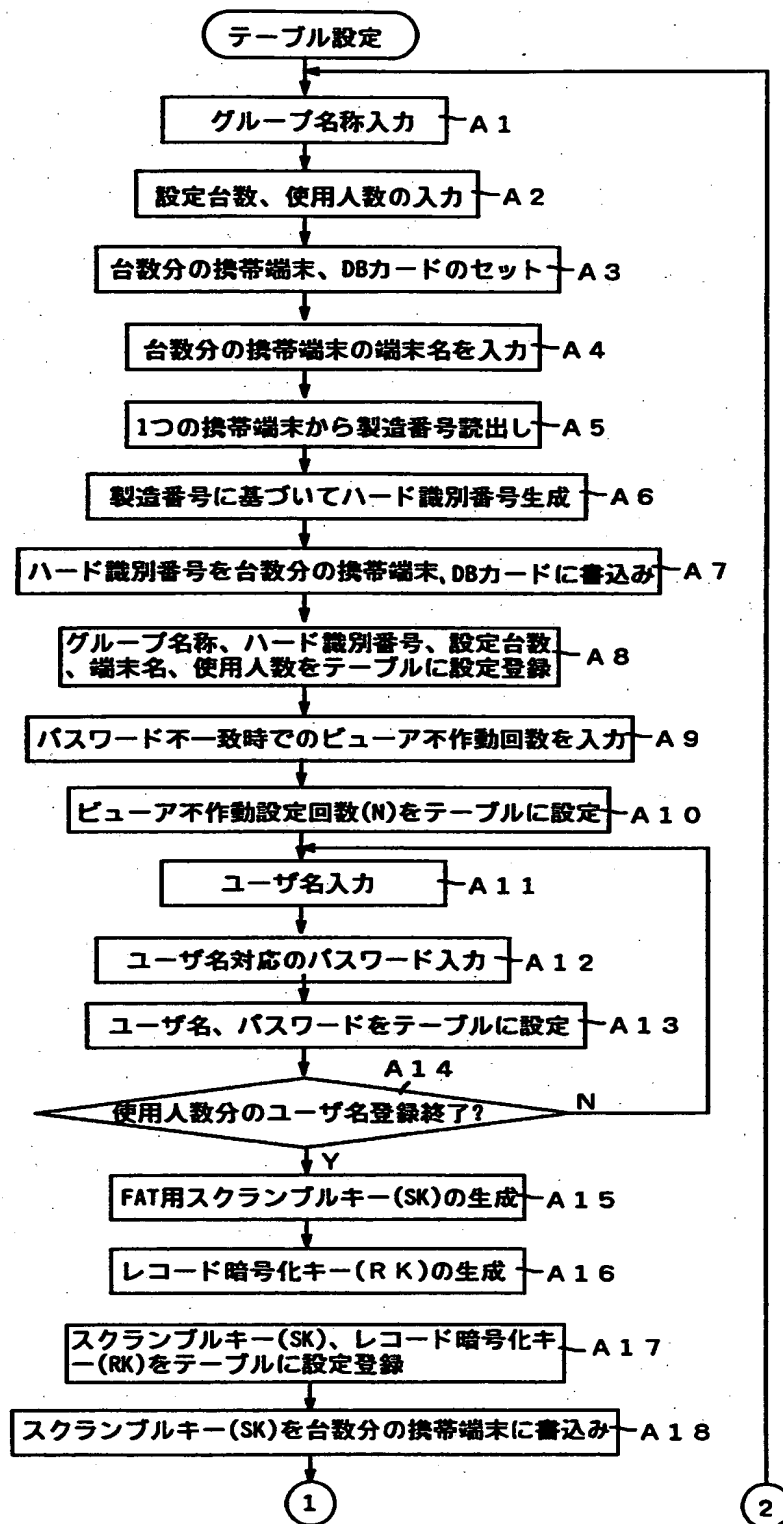
FlashROM	
	ハード識別番号
	ソフト識別番号
	スクランブルキー (SK)
RAM (一次記憶メモリ)	
	キー/データ入力エリア
	FAT読出しエリア
	レコードエリア
	その他

【図 7】

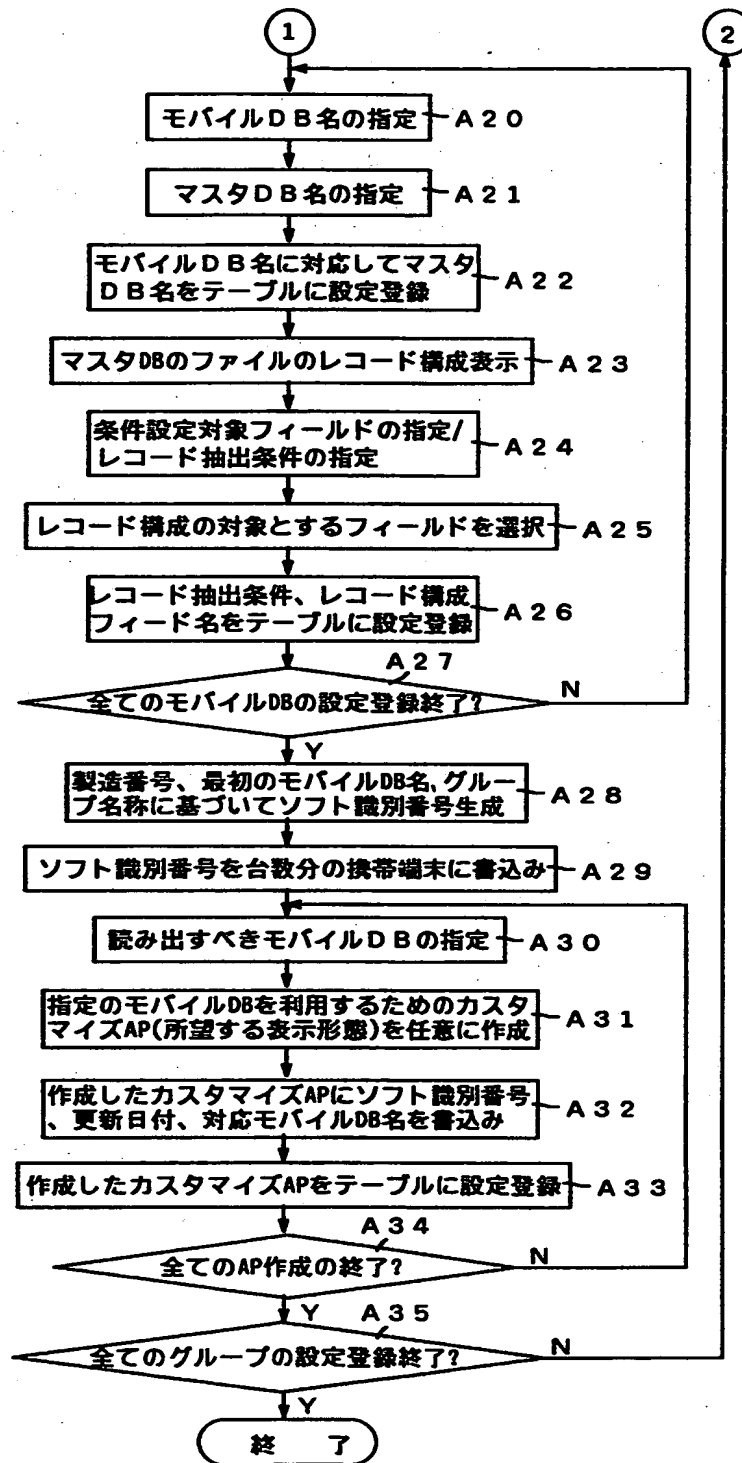
サーバ/端末ブロック図



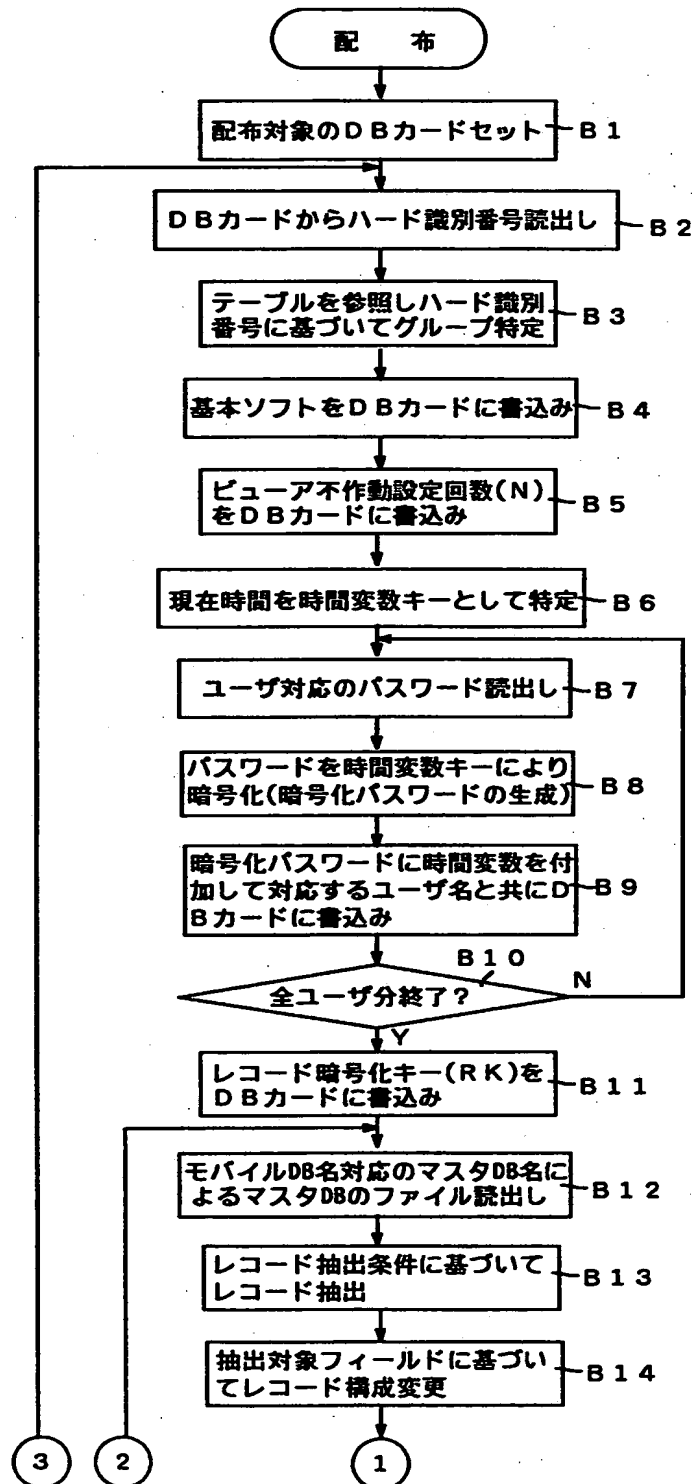
【図 8】



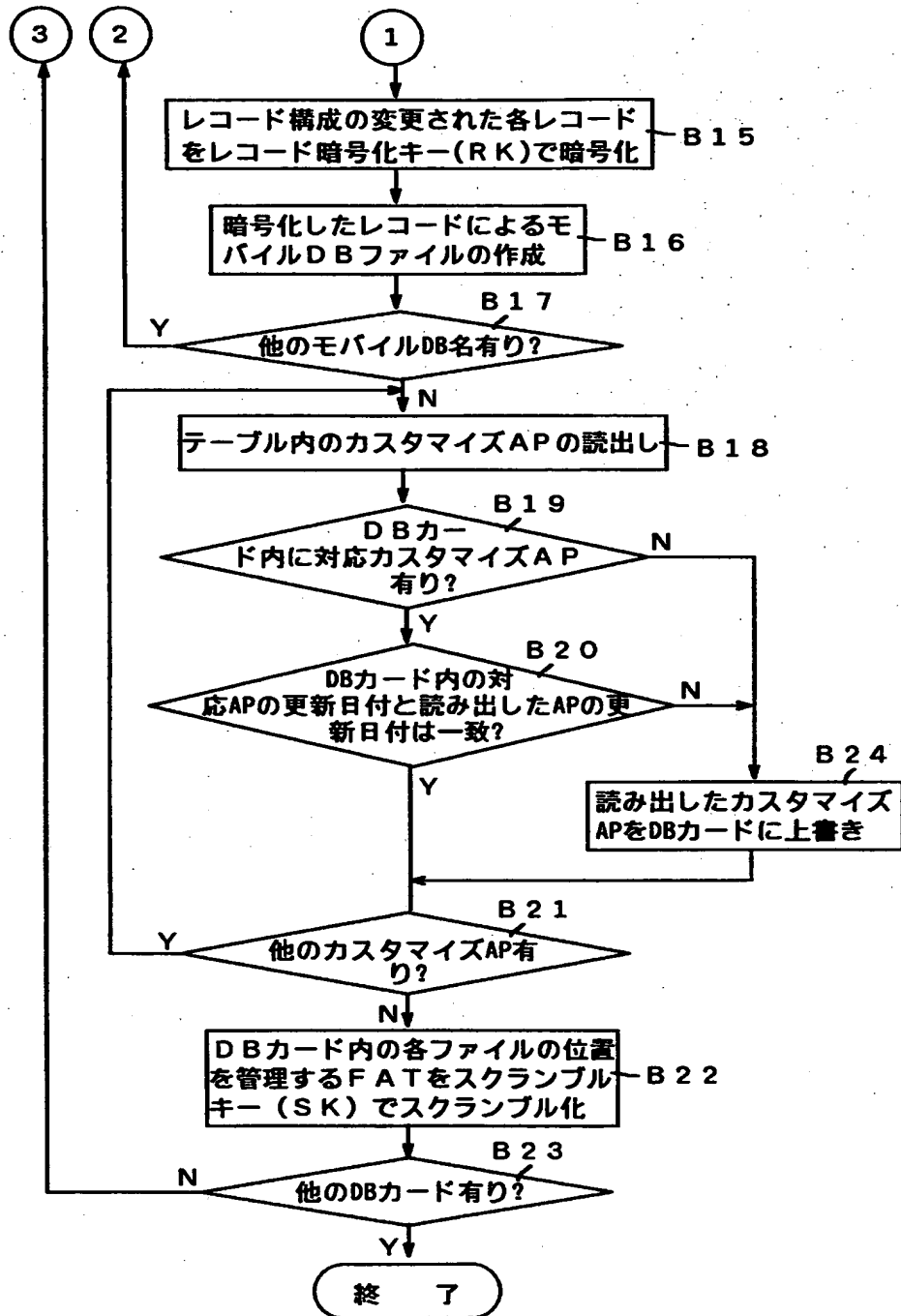
【図 9】



【図10】



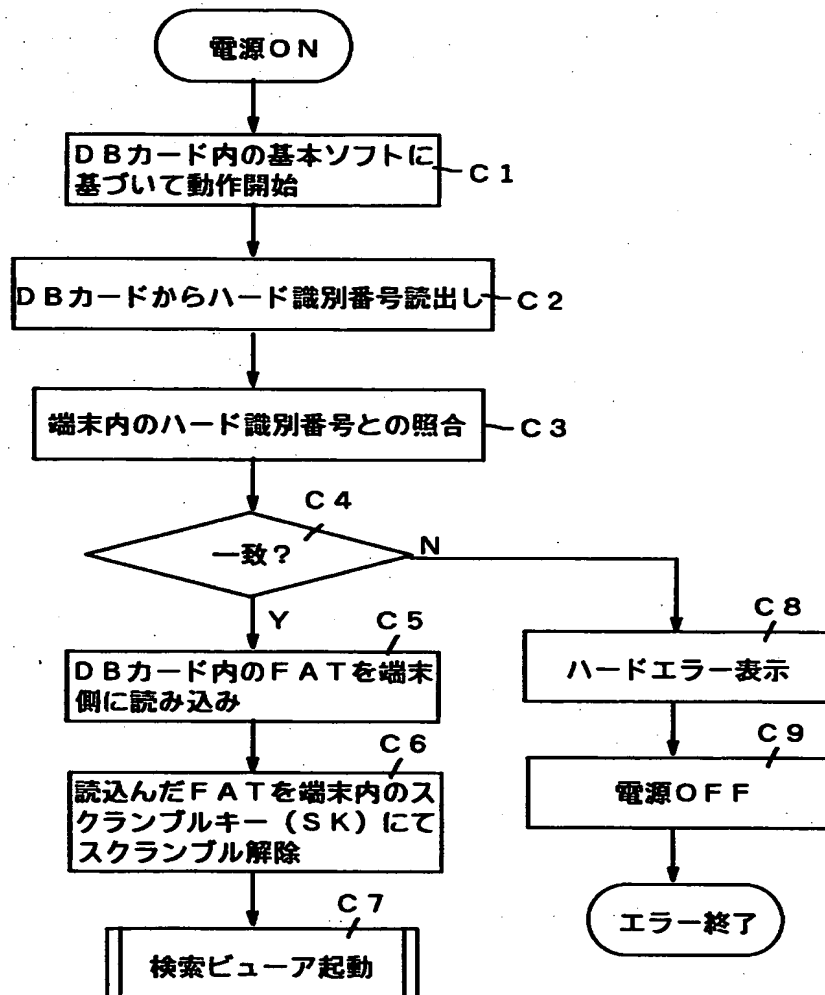
【図 11】



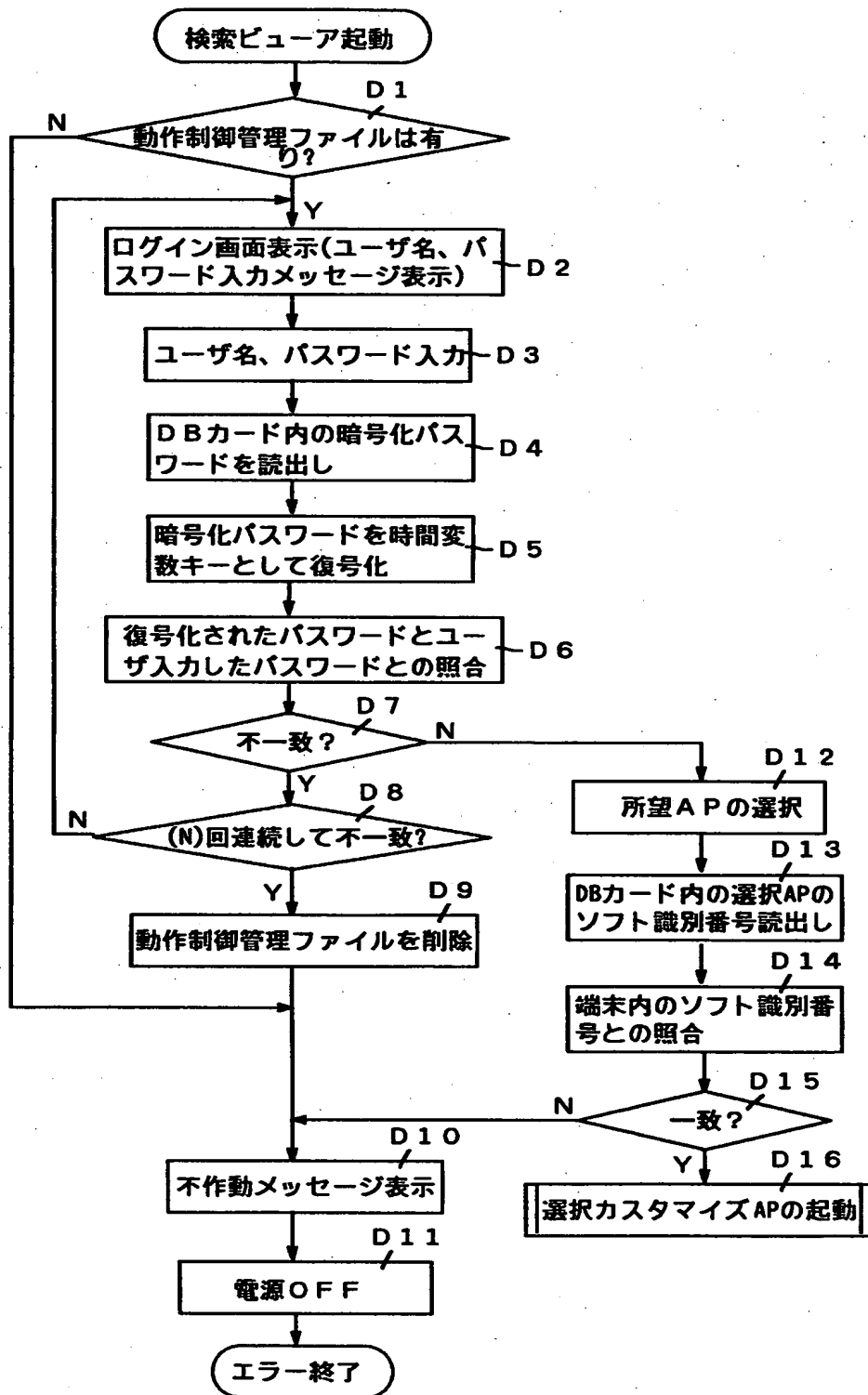
【図12】

		マスタDB							
(A)		A	B	C	D	E	F	G	H
	1								
	2								
	3								
	4								
	5								
	6								
	7								
	8								
	9								
	10								
		レコード抽出							
(B)		A	B	C	D	E	F	G	H
	1								
	2								
	3								
	4								
	5								
		レコード構成変更				モバイルDBの完成			
(C)		A	B	E	G				
	1								
	2								
	3								
	4								
	5								

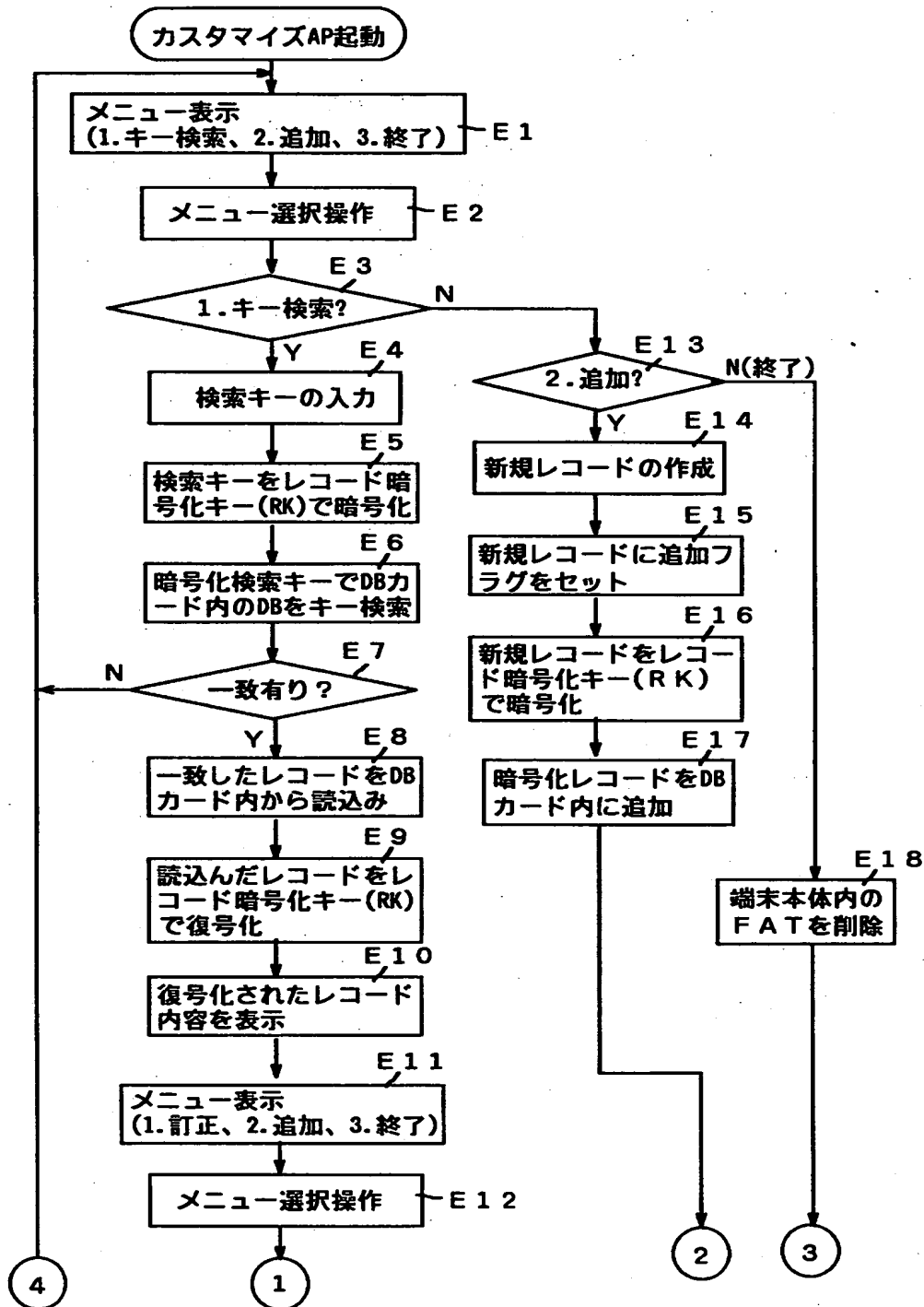
【図 1 3】



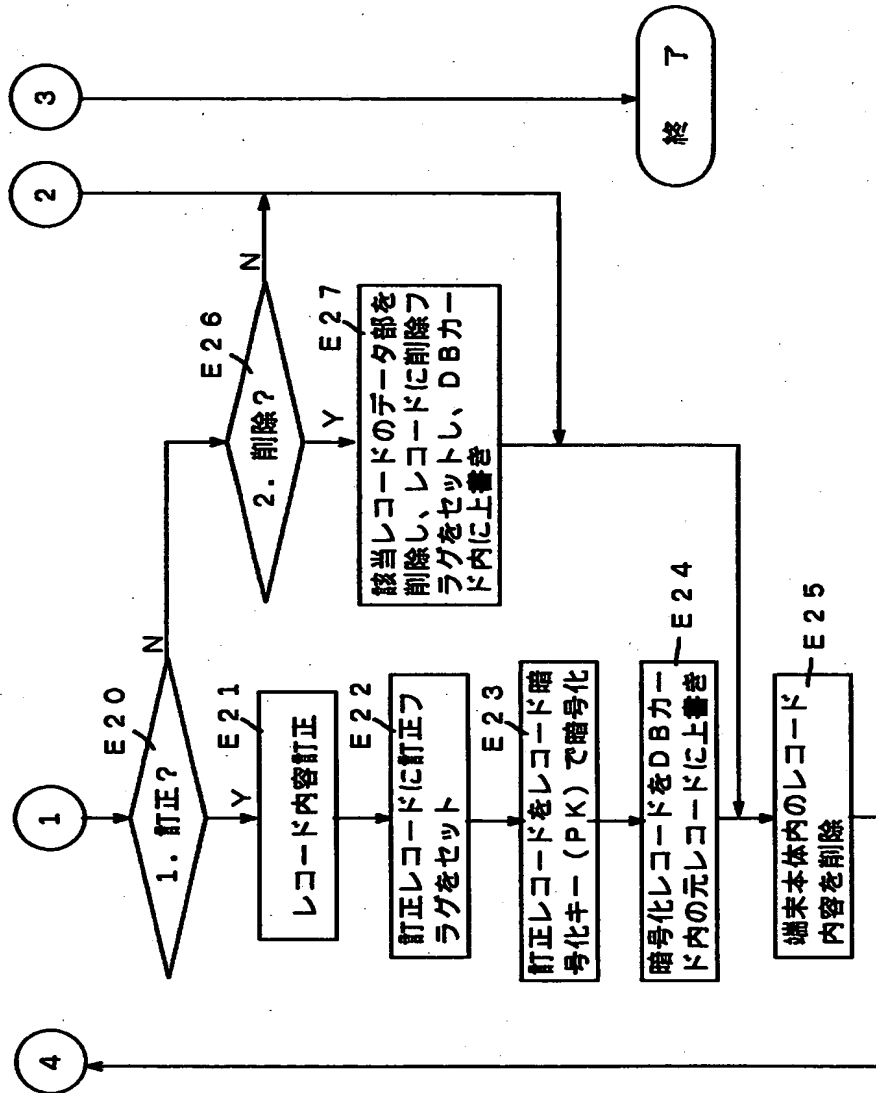
【図14】



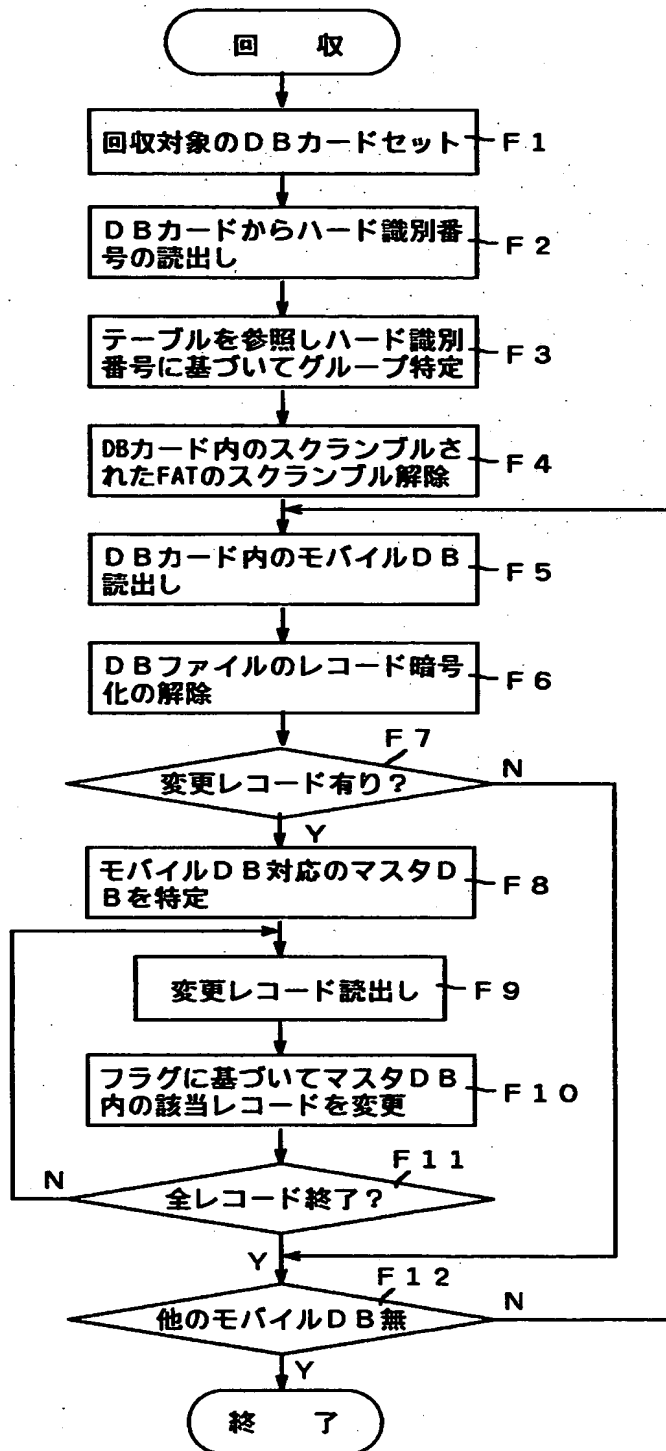
【図15】



【図 16】



【図 17】



【書類名】 要約書

【要約】

【課題】元となるマスタDBをそのまま書き込むのではなく、マスタDBから切り出したレコード群のみからなるモバイルDBを作成して書き込むことで、当該カード対応の正当な端末に対しても必要以上の情報を提供しないという対策を講じることができ、紛失、盗難、悪意等によるデータ記憶媒体内の重要情報の漏洩を確実に防止することができる。

【解決手段】サーバ装置1はDBカード3へのデータファイルの書き込みの他、そのカードとそれをアクセス可能な携帯端末装置2との対応付けを一括して行う。そして、マスタDBから切り出したレコード群のみからなるモバイルDBを作成してカードへ書き込む。携帯端末装置2は端末とカードとの対応付けにより、正当なカードであれば、そのモバイルDBに対するアクセスを許可する。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2000-004271
受付番号	50000021877
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 1月14日

<認定情報・付加情報>

【提出日】	平成12年 1月13日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000001443]

1. 変更年月日 1998年 1月 9日

[変更理由] 住所変更

住 所 東京都渋谷区本町1丁目6番2号

氏 名 カシオ計算機株式会社